N/REF: 0020/2022

Examinada su solicitud de informe, remitida a este Gabinete Jurídico, referente al Anteproyecto de Ley reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción por la que se transpone la Directiva (UE) 2019/1937 del Parlamento Europeo y del Consejo, de 23 de octubre de 2019, relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión, solicitado, con carácter urgente, de esta Agencia Española de Protección de Datos (AEPD) de conformidad con lo dispuesto en el artículo 47 de la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de los derechos digitales (LOPDGDD), en relación con el artículo 57.1, letra c), del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales, y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos), y 5 b) del Estatuto de la Agencia, aprobado por Real Decreto 389/2021, de 1 de junio, cúmpleme informarle lo siguiente:

Antes de entrar a analizar el texto sometido a informe es preciso señalar que, habida cuenta de la fundamentación legal del informe que inmediatamente va a evacuarse y su carácter preceptivo, a tenor de lo dispuesto en las normas que acaban de señalar, debería indicarse en la Exposición de Motivos de la norma que la misma ha sido sometida al previo informe de la Agencia Española de Protección de Datos.

El anteproyecto remitido tiene por objeto otorgar protección adecuada frente a las represalias que puedan sufrir las personas físicas que informen, a través de los procedimientos previstos en la misma, alguna de los acciones u omisiones incluidas en su ámbito de aplicación y procede a la transposición al ordenamiento interno la Directiva (UE) 2019/1937, del Parlamento Europeo y del Consejo, de 23 de octubre de 2019, relativa a la protección de las personas que informen sobre infracciones de Derecho de la Unión.

Dicha Directiva parte de la relevancia que tienen las denuncias y revelaciones públicas hechas por los denunciantes para garantizar el cumplimiento del Derecho y de las políticas de la Unión, por lo que, encontrándose fragmentada y siendo desigual en los distintos ámbitos la protección de los denunciantes en la Unión, establece unas normas mínimas comunes que garanticen una protección efectiva de los denunciantes en lo que respecta a aquellos ámbitos que la misma identifica, sin perjuicio de la facultad de los Estados miembros de poder decidir hacer extensiva la aplicación de las

disposiciones nacionales a otros ámbitos con el fin de garantizar que exista un marco global y coherente de protección de los denunciantes a escala nacional. A estos efectos, la Directiva establece una serie de garantías, que deben considerarse como un régimen de mínimos, dirigidas a proteger a los informantes, estableciendo un régimen de comunicación de la información que se articula por tres vías: los sistemas internos, los canales externos y la revelación pública.

Asimismo debe tenerse en cuenta que, previamente a la aprobación de la Directiva (UE) 2019/1937, ya existía en el ordenamiento jurídico español una normativa general (sin perjuicio de la normativa especial existente en los sectores específicos en los que así estaba ya previsto) sobre los sistemas de información de denuncias internas en el sector privado, recogida en el artículo 24 de la LOPDGDD:

> *Artículo 24. Sistemas de información de denuncias internas.*
>
> *1. Será lícita la creación y mantenimiento de sistemas de información a través de los cuales pueda ponerse en conocimiento de una entidad de Derecho privado, incluso anónimamente, la comisión en el seno de la misma o en la actuación de terceros que contratasen con ella, de actos o conductas que pudieran resultar contrarios a la normativa general o sectorial que le fuera aplicable. Los empleados y terceros deberán ser informados acerca de la existencia de estos sistemas de información.*
>
> *2. El acceso a los datos contenidos en estos sistemas quedará limitado exclusivamente a quienes, incardinados o no en el seno de la entidad, desarrollen las funciones de control interno y de cumplimiento, o a los encargados del tratamiento que eventualmente se designen a tal efecto. No obstante, será lícito su acceso por otras personas, o incluso su comunicación a terceros, cuando resulte necesario para la adopción de medidas disciplinarias o para la tramitación de los procedimientos judiciales que, en su caso, procedan.*
>
> *Sin perjuicio de la notificación a la autoridad competente de hechos constitutivos de ilícito penal o administrativo, solo cuando pudiera proceder la adopción de medidas disciplinarias contra un trabajador, dicho acceso se permitirá al personal con funciones de gestión y control de recursos humanos.*
>
> *3. Deberán adoptarse las medidas necesarias para preservar la identidad y garantizar la confidencialidad de los datos correspondientes a las personas afectadas por la información suministrada, especialmente la de la persona que hubiera puesto los hechos en conocimiento de la entidad, en caso de que se hubiera identificado.*
>
> *4. Los datos de quien formule la comunicación y de los empleados y terceros deberán conservarse en el sistema de denuncias*

únicamente durante el tiempo imprescindible para decidir sobre la procedencia de iniciar una investigación sobre los hechos denunciados.

En todo caso, transcurridos tres meses desde la introducción de los datos, deberá procederse a su supresión del sistema de denuncias, salvo que la finalidad de la conservación sea dejar evidencia del funcionamiento del modelo de prevención de la comisión de delitos por la persona jurídica. Las denuncias 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 esta ley orgánica.

Transcurrido el plazo mencionado en el párrafo anterior, los datos podrán seguir siendo tratados, por el órgano al que corresponda, conforme al apartado 2 de este artículo, la investigación de los hechos denunciados, no conservándose en el propio sistema de información de denuncias internas.

5. Los principios de los apartados anteriores serán aplicables a los sistemas de denuncias internas que pudieran crearse en las Administraciones Públicas.

Se procedía, de este modo, a la regulación de una materia que no había sido objeto de regulación específica con anterioridad, sin perjuicio de la existencia de diversos dictámenes de la Agencia Española de Protección de Datos, así como del Grupo de Trabajo creado por el artículo 29 de la Directiva 95/46/CE que se referían a este tipo de tratamientos.

De este modo, la existencia de unos canales de denuncia de incumplimientos internos o de actividades ilícitas de la empresa se justificaba en el régimen de responsabilidad penal de las personas jurídicas introducido en el artículo 31 bis del Código Penal por la reforma operada por la Ley Orgánica 1/2015, de 30 de marzo y en la interpretación de sus requisitos por la Circular 1/2016, de la Fiscalía General del Estado, que consideraba a estos canales como uno de los elementos clave de los modelos de prevención. Por ello, resultaba necesario el establecimiento de un régimen que regulara los sistemas de denuncia interna de estos ilícitos en el que se recogieran las garantías esenciales del derecho fundamental a la protección de datos, cuyo tratamiento, tal y como argumentó el Consejo de Estado en su Dictamen 757/2017, sobre el Anteproyecto de Ley Orgánica de Protección de Datos de Carácter Personal, quedaba legitimado por “la existencia de un interés público legitimador de estos tratamientos”.

I

El anteproyecto objeto de informe tiene una especial trascendencia desde la perspectiva de la protección de datos personales, debiendo ajustarse a las previsiones contenidas en 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), plenamente aplicable desde el 25 de mayo de 2018, así como a la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y, en su caso, a la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, tal y como se recoge expresamente en el artículo 29 del anteproyecto.

En este sentido, destacan las numerosas referencias que, a este respecto, se contienen en la Directiva (UE) 2019/1937 que, además de incluir la protección de los datos personales dentro de los ámbitos de aplicación material (artículo 2.1.x.), cita en reiteradas ocasiones la aplicación de su normativa específica (Considerandos 83, 84 y 85 y artículo 17), e introduce garantías específicas dirigidas a su protección (anonimato, confidencialidad, minimización, formación específica y otras que se analizarán a lo largo del presente informe).

Asimismo, debe recordarse que la regulación de la Directiva es “de mínimos” (Considerando 5 y artículo 1), por lo que los Estados miembros pueden establecer garantías adicionales dirigidas a la protección efectiva de los denunciantes; igualmente, corresponde a los Estados miembros velar por la aplicación de la normativa de protección de datos personales respecto de los distintos sujetos cuyos datos personales puedan ser objeto de tratamiento, y a los que posteriormente nos referiremos (Considerandos 76, 83, 84 y 85), prestando especial a los principios establecidos en el artículo 5 del RGPD y en el artículo 4 de la Directiva (UE) 2016/680 y al principio de protección de datos desde el diseño y por defecto del artículo 25 del RGPD y 20 de la Directiva (UE) 2016/680 y, en su caso, al perseguir los procedimientos previstos en la Directiva “un objetivo importante de interés público de la Unión y de los Estados miembros”, mediante la restricción de determinados derechos de protección de datos de las personas afectadas al amparo del artículo 23 del RGPD y 13, 15 y 16 de la Directiva (UE) 2016/680.

Esta especial incidencia en los tratamientos de datos personales se refleje en el texto remitido, el cual dedica un título específico, el Título VI, a la “Protección de datos personales”, que comprende los artículos 29 a 34, y cuya inclusión se valora muy positivamente por esta Agencia, sin perjuicio de las observaciones que se realizan a lo largo del presente informe.

Sin embargo, no se analizan con el detalle necesario en la Memoria de Análisis de Impacto Normativo los distintos tratamientos de datos personales que pueden realizarse al amparo de esta norma, ni se justifican determinadas opciones que adopta el legislador, como las relativas al acceso a los datos

personales o las limitaciones que la misma establece. Asimismo, hubiera sido deseable una descripción del funcionamiento de los canales de denuncia con el objeto de facilitar la identificación de las garantías que resulten necesarias para la adecuada tutela del derecho fundamental a la protección de datos personales.

A este respecto, teniendo en cuenta que el tratamiento de datos personales viene impuesto o legitimado por el Derecho de la Unión y de los Estados miembros, y dentro del margen de apreciación que deja la Directiva y al objeto de su adecuada incorporación a nuestro ordenamiento jurídico, procede recordar el criterio que viene reiterando esta Agencia al informar los proyectos de ley que tienen una especial incidencia en el tratamiento de datos personales, respecto a la necesidad de evaluar adecuadamente su impacto y poder adoptar las garantías legales oportunas.

En este sentido, en el Informe 86/2021, referente al Anteproyecto de Ley Orgánica por la que se modifican la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, para la transposición de directivas en materia de lucha contra el fraude y la falsificación de medios de pago distintos del efectivo y de abuso de mercado, y la Ley Orgánica 7/2014, de 12 de noviembre, sobre intercambio de información de antecedentes penales y consideración de resoluciones judiciales penales en la Unión Europea, recordábamos lo siguiente:

> Tal y como resulta del apartado anterior, los tratamientos de datos personales por el Sistema de Registros queda sujeto a la normativa general sobre protección de datos de carácter personal, y en la medida en que los mismos se fundamentarán en el cumplimiento de una misión de interés público o de obligaciones legales, su régimen deberá establecerse por una norma con rango de ley, tal y como resulta de las previsiones del RGPD y la LOPDGDD y de la jurisprudencia del TJUE y de nuestro Tribunal Constitucional.
>
> A este respecto, el artículo 8 de la LOPDGDD recoge el principio constitucional de reserva de ley:
>
> > Artículo 8. Tratamiento de datos por obligación legal, interés público o ejercicio de poderes públicos.
> > 1. El tratamiento de datos personales solo podrá considerarse fundado en el cumplimiento de una obligación legal exigible al responsable, en los términos previstos en el artículo 6.1.c) del Reglamento (UE) 2016/679, cuando así lo prevea una norma de Derecho de la Unión Europea o una norma con rango de ley, que podrá determinar las condiciones generales del tratamiento y los tipos de datos objeto del mismo así como las cesiones que procedan como consecuencia del cumplimiento de la obligación legal. Dicha norma podrá igualmente imponer condiciones

especiales al tratamiento, tales como la adopción de medidas adicionales de seguridad u otras establecidas en el capítulo IV del Reglamento (UE) 2016/679.
2. El tratamiento de datos personales solo podrá considerarse fundado en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable, en los términos previstos en el artículo 6.1 e) del Reglamento (UE) 2016/679, cuando derive de una competencia atribuida por una norma con rango de ley

Asimismo, deberá tenerse en cuenta la doctrina constitucional recogida, fundamentalmente en las citadas 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, de modo que dicha norma con rango de ley *"ha de reunir todas aquellas características indispensables como garantía de la seguridad jurídica», esto es, «ha de expresar todos y cada uno de los presupuestos y condiciones de la intervención» (STC 49/1999, FJ 4). En otras palabras, «no sólo excluye apoderamientos a favor de las normas reglamentarias […], sino que también implica otras exigencias respecto al contenido de la Ley que establece tales límites» (STC 292/2000, FJ 15).*

Asimismo, deberá establecer 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.

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:

> 65 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 [véase, en este sentido, el dictamen 1/15 (Acuerdo PNR UE-Canadá), de 26 de julio de 2017, EU:C:2017:592, apartados 140 y 141 y jurisprudencia citada).

Partiendo de las normas y de la doctrina jurisprudencial citada, esta Agencia viene señalando en sus informes más recientes la necesidad de que, por parte del legislador, al introducir regulaciones en nuestro ordenamiento jurídico que tengan especial trascendencia en los tratamientos de datos de carácter personal, se proceda previamente a un análisis de los riesgos que puedan derivarse de los mismos, incluyendo en la Memoria de Análisis de Impacto Normativo un estudio sistematizado del impacto que en el derecho fundamental a la protección de datos personales de los interesados han de tener los distintos tratamientos de datos que prevé la ley. En este sentido se han pronunciado el Informe 77/2020, relativo al Anteproyecto de Ley Orgánica de Lucha contra el Dopaje en el Deporte o el Informe 74/2020 referido al Anteproyecto de Ley de memoria democrática.

Como consecuencia de lo indicado, esta Agencia considera necesario que se realice, con intervención del delegado de protección de datos del Ministerio de Justicia, un análisis de riesgos y, en su caso, una Evaluación de impacto en la protección de datos, que permita identificar las garantías necesarias que habría que trasladar al presente texto legal.

Asimismo, dada la trascendencia que tiene la garantía del derecho fundamental a la protección de datos personales y con la finalidad de permitir que las disposiciones normativas que se tramitan recojan las garantías específicas que resulten necesarias, esta Agencia considera necesario que se impulse una modificación del Real Decreto 931/2017, de 27 de octubre, por el que se regula la Memoria del Análisis de Impacto Normativo, con el fin de que se incluyan, tanto en el contenido de la memoria de análisis de impacto normativa como en el de la memoria abreviada, el impacto en la protección de datos personales.

Por otro lado, en relación con la aplicación de la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales, que ha procedido a la transposición de la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, debe recordarse que la misma establece un régimen especial que ha de ser objeto de interpretación restrictiva, tal y como se señaló reiteradamente en nuestro Informe 29/2020 sobre el Anteproyecto dicha Ley Orgánica, recordando que la Directiva

> "viene a configurar un régimen especial, al que se someterían únicamente los tratamientos que la misma regula, frente al régimen general de protección de datos que se recoge en el Reglamento general de protección de datos. Por este motivo, las disposiciones del mismo serán de aplicación a todos los tratamientos llevados a cabo dentro del ámbito de aplicación del derecho de la Unión y que no estén regulados específicamente por la Directiva, tal y como se desprende del ámbito de aplicación establecido en el artículo 2 del Reglamento".

De este modo, y de acuerdo con los artículos 1 y 2 de la Directiva, la misma se aplica al tratamiento de datos personales por parte de las autoridades competentes a los 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 contra la seguridad pública, debiendo interpretarse este último inciso en relación con las que tengan naturaleza penal, quedando excluidas la de carácter administrativo. Por consiguiente, se configuran dos requisitos cumulativos, que se trate de tratamientos realizados por quien ostente la condición de autoridad competente y para los fines señalados, de modo que faltando alguno de ellos, no se trataría de una norma de transposición de la Directiva y estaría extendiendo a supuestos no contemplados en la misma una regulación más restrictiva del derecho fundamental a la protección de datos personales que la establecida en el RGPD, que sería la norma general aplicable a los tratamientos en los que no concurran esos requisitos. Todo ello sin perjuicio de que, al amparo del artículo 23 del RGPD y siempre que se justifique la concurrencia de alguno de los supuestos previstos en el mismo, puedan establecerse limitaciones a los derechos de los afectados, que deberán responder al principio de proporcionalidad, pero sin que sea extensible, sin más, una regulación más restrictiva prevista para un supuesto diferente, como es la contenida en la Directiva.

Por consiguiente, la misma únicamente resultará de aplicación en cuanto se trate de tratamientos de datos personales realizados por las autoridades competentes designadas en la Ley Orgánica 7/2021 y a los fines determinados en la misma, por lo que, cuando se trate de supuestos de colaboración con

dicha autoridades competentes, y como señalábamos en nuestro informe 29/2020:

> "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".

II

Sin perjuicio de lo anterior, procede analizar las principales cuestiones que, en materia de protección de datos personales, suscita el texto remitido, si bien con la concisión propia de la urgencia con la que el mismo se solicita.

A este respecto, pueden identificarse las siguientes cuestiones: posición jurídica de los intervinientes en el tratamiento de los datos personales; sujetos cuyos datos personales pueden ser objeto de tratamiento; base jurídica; aplicación de los principios de protección de datos y limitaciones a los derechos de los afectados.

Comenzando con la posición jurídica de los intervinientes en el tratamiento de los datos personales, debe partirse de la definición de «responsable del tratamiento» contenida en el artículo 4.7. del RGPD: *la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros;* Así como la de «encargado del tratamiento del artículo 4.8. del RGPD: *la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento*.

En el sistema interno de información, los fines y los medios del tratamiento vendrían determinados por la ley, estableciendo en el artículo 5.1. del anteproyecto que *"El órgano de administración u órgano de gobierno de cada entidad u organismo obligado por la presente ley será el responsable de la implantación del sistema interno de información, previa consulta con la representación legal de las personas trabajadoras"*, y definiendo, en su apartado 2 los requisitos que deberán cumplir dichos sistemas *en cualquiera de sus fórmulas de gestión:*

2. Los sistemas internos de información, en cualquiera de sus fórmulas de gestión, deberán:

a) Permitir comunicar información sobre las infracciones previstas en el artículo 2 a todas las personas referidas en el artículo 3.

b) Estar diseñados, establecidos y gestionados 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, la protección de datos, impidiendo el acceso de personal no autorizado.

c) Permitir la presentación de comunicaciones por escrito o verbalmente, o de ambos modos.

d) Integrar los distintos canales internos de comunicación que pudieran establecerse dentro de la entidad.

e) Garantizar que las comunicaciones presentadas puedan tratarse de manera efectiva dentro de la correspondiente entidad u organismo con el objetivo de que el primero en conocer la posible irregularidad sea el propio empleador.

f) Ser independientes y aparecer diferenciados respecto de los sistemas internos de información de otras entidades u organismos, sin perjuicio de lo establecido en los artículos 12 y 13 siguientes.

g) Contar con un responsable del Sistema en los términos previstos en el artículo 10 de esta ley.

h) Contar con una política o estrategia que enuncie los principios generales en materia de sistemas internos de información y defensa del informante y que sea debidamente publicitada en el seno de la entidad u organismo.

i) Contar con un procedimiento de gestión de las comunicaciones recibidas. J

) 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.

Por consiguiente, en virtud de las funciones que se le atribuyen legalmente, corresponde al órgano de administración u órgano de gobierno de cada entidad u organismo obligado ostentar la condición de «responsable del tratamiento» de los datos personales, de conformidad con lo dispuesto en la normativa sobre protección de datos personales, lo que debería recogerse en texto del propio artículo 5.

En este punto, el anteproyecto de ley permite compartir medios tanto en el artículo 12, respecto del sector privado, como en el artículo 14 respecto del sector público. En estos casos, en virtud de cómo se articule esa colaboración, podríamos encontrarnos ante la figura de la corresponsabilidad a la que se refiere el artículo 26 del RGPD, prevista para los supuestos en que “dos o más responsables determinen conjuntamente los objetivos y los medios del

tratamiento serán considerados corresponsables del tratamiento" o, por el contrario, ante un supuesto de responsables respectivos respecto de los tratamientos de datos personales que realicen. Por lo tanto, en opinión de esta Agencia, no se puede determinar, a priori, la posición jurídica que corresponderá a cada uno de los responsables del tratamiento. No obstante, se recuerda que, en el caso de que se articule una corresponsabilidad desde la perspectiva de protección de datos personales, deberá suscribirse el acuerdo al que se refiere el citado artículo 26 del RGPD.

Por otro lado, el artículo 6 del anteproyecto regula la «gestión del anteproyecto por tercero externo», el cual tendría la consideración de encargado del tratamiento, como adecuadamente se establece en el propio texto remitido, en el cual se establece la obligación específica de que el mismo ofrezca garantías adecuadas de respeto de la protección de datos (requisito imprescindible al amparo del artículo 28.1. del RGPD):

> *Artículo 6. Gestión del sistema por tercero externo.*
>
> *1. La gestión de los sistemas internos de información se podrá llevar a cabo dentro de la propia entidad u organismo o acudiendo a un tercero externo, en los términos previstos en esta ley. A estos efectos, se considera gestión del sistema la recepción de informaciones.*
>
> *2. La gestión del sistema por un tercero externo exigirá en todo caso que éste ofrezca garantías adecuadas de respeto de la independencia, la confidencialidad, la protección de datos y el secreto.*
>
> *3. La gestión del sistema interno de información por un tercero no podrá suponer un menoscabo de las garantías y requisitos que para dicho sistema establece la presente ley ni una atribución de la responsabilidad sobre el mismo en persona distinta del Responsable del Sistema.*
>
> *4. El tercero externo que gestione el canal tendrá la consideración de encargado del tratamiento a efectos de la legislación sobre protección de datos personales.*

El citado precepto plantea dudas respecto de su alcance, al limitar, en principio, la gestión del sistema que se puede externalizar a "la recepción de informaciones", lo que implicaría que dicha previsión actuaría como límite o garantía específica, por lo que únicamente podrían externalizarse los tratamientos de datos personales correspondientes a la mera recepción de las informaciones y a su comunicación al órgano competente para su tramitación. No obstante, el artículo 8, al regular el procedimiento de gestión de comunicaciones, incluye otras actuaciones como el envío de acuse de recibo, la posibilidad mantener comunicación con el informante y solicitarle información adicional o su derecho, así como el de las personas investigadas, a ser oídas en el procedimiento y el artículo 12 del anteproyecto, al regular los medios compartidos, hace una referencia conjunta a la "gestión y tramitación de las

comunicaciones, tanto si la gestión del sistema se lleva a cabo por la propia entidad como si se ha externalizado", lo que parece dar a entender que el ámbito de actuación de terceros puede ser mayor, pudiendo ser objeto de externalización tanto la gestión como la tramitación. Por el contrario, en el artículo 15 del anteproyecto, se prevé expresamente que la externalización de la gestión del sistema interno de información en el sector público "comprenderá únicamente el procedimiento para la recepción de las informaciones sobre infracciones".

Por otro lado, al regular en el artículo 9 la figura del Responsable del Sistema, parece diferenciarse en el apartado 2 entre "gestión del sistema interno de información" y "tramitación de expedientes de investigación" debiendo recaer dichas funciones, en el sector privado y conforme al apartado 5 del citado artículo 9, en un alto directivo de la entidad, lo que implicaría que las funciones de tramitación de expedientes, no serían susceptibles de externalización al haberse limitado la misma, por el artículo 6, únicamente a la gestión del sistema, entendiendo por tal la recepción de informaciones.

El Considerando 54 de la Directiva (UE) 2019/1937 se refiere expresamente a la posibilidad de externalización en los siguientes términos: "También se puede autorizar a terceros a recibir denuncias de infracciones en nombre de entidades jurídicas de los sectores privado y público, siempre que ofrezcan garantías adecuadas de respeto de la independencia, la confidencialidad, la protección de datos y el secreto. Dichos terceros pueden ser proveedores de plataformas de denuncia externa, asesores externos, auditores, representantes sindicales o representantes de los trabajadores". Aunque el citado considerando se refiere a la recepción de las denuncias, el artículo 8 de la Directiva prevé en su apartado 5 que "Los canales de denuncia podrán gestionarse internamente por una persona o departamento designados al efecto o podrán ser proporcionados externamente por un tercero" y en el apartado 6 que "Las entidades jurídicas del sector privado que tengan entre 50 y 249 trabajadores podrán compartir recursos para la recepción de denuncias y toda investigación que deba llevarse a cabo". Y el artículo 9.1.c) señala que "Los procedimientos de denuncia interna y seguimiento a que se refiere el artículo 8 incluirán lo siguiente: c) la designación de una persona o departamento imparcial que sea competente para seguir las denuncias, que podrá ser la misma persona o departamento que recibe las denuncias y que mantendrá la comunicación con el denunciante y, en caso necesario, solicitará a este información adicional y le dará respuesta".

A juicio de esta Agencia, no existe una regulación clara en el anteproyecto de ley respecto de las actuaciones que pueden ser objeto de externalización, lo que puede generar inseguridad jurídica y, desde la perspectiva de la protección de datos personales, limitar los tratamientos de datos personales que pueden ser realizados por un encargado del tratamiento. La regulación a este respecto que se realiza en el artículo 32, al incluir entre los

sujetos que pueden acceder a los datos personales, a los encargados del tratamiento, no es clarificadora al respecto, ya que se limita al ámbito de “sus competencias y funciones”, que, al menos en este punto, suscitan las dudas señaladas.

Por consiguiente, debe aclararse en el artículo 6 las actuaciones que pueden ser objeto de externalización clarificando si se limita a la recepción de informaciones o también a otras actuaciones, incluyendo o no la tramitación de las mismas y adaptando, en su caso, el artículo 12, con el objeto de que no existan dudas respecto de los tratamientos de datos personales que se pueden encomendar a un encargado del tratamiento.

Por otro lado, en relación con el encargado del tratamiento, el artículo 28.3. del RGPD prevé que “El tratamiento por el encargado se regirá por un contrato u otro acto jurídico con arreglo al Derecho de la Unión o de los Estados miembros, que vincule al encargado respecto del responsable y establezca el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable” detallando a continuación el contenido particular del mismo. **Por ello, debe incluirse en el apartado 4 del artículo 6 la necesidad de suscribir el acto o contrato al que se refiere el artículo 28.3 del RGPD**.

En el caso del sector público, no resulta necesario hacer referencia a dicho acto o contrato, al encontrarse dicha previsión recogida en la disposición adicional vigésima quinta de 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, si bien las remisiones que realiza la LCSP, al ser anterior a la plena aplicación del RGPD, se realizan a la LOPD de 1999, por lo que dichas remisiones deben entenderse hechas al RGPD.

Por último, procede hacer referencia a la figura del responsable del correcto funcionamiento del sistema y que, bajo la denominación de “responsable del sistema interno de información”, se regula en el artículo 9 del anteproyecto, y entre cuyas funciones se encuentra la de aprobar el procedimiento de gestión de comunicaciones. En este caso, de la regulación del artículo 9, que prevé su designación por el órgano de administración u órgano de gobierno de cada entidad u organismo obligado, es decir, desde la perspectiva de la protección de datos personales, por el responsable del tratamiento, resulta que el mismo debe ser un alto directivo, por lo que, en el supuesto en que tenga que acceder a los datos personales, el mismo no tendrá la consideración de encargado sino que accederá en el ejercicio de sus funciones y en su condición de personal del propio responsable.

En lo que se refiere al Canal externo de comunicaciones, el anteproyecto prevé la creación de la Autoridad Independiente de Protección del Informante, a

la que atribuye las correspondientes competencias, por lo que la misma ostentará la condición de responsable de los tratamientos de datos personales que realice.

III

Procede, a continuación, hacer referencia a los distintos sujetos cuyos datos personales pueden ser objeto de tratamiento.

A este respecto, debe partirse de que la finalidad primaria de la norma es proteger a los informantes, que la Directiva define como “una persona física que comunica o revela públicamente información sobre infracciones obtenida en el contexto de sus actividades laborales”.

La Directiva (UE) 2019/1937 contempla la posibilidad de que la información se facilite de forma anónima, a la que se refieren expresamente los apartados 2 y 3 de su artículo 6:

> *2. Sin perjuicio de la obligación vigente de disponer de mecanismos de denuncia anónima en virtud del Derecho de la Unión, la presente Directiva no afectará a la facultad de los Estados miembros de decidir si se exige o no a las entidades jurídicas de los sectores privado o público y a las autoridades competentes aceptar y seguir las denuncias anónimas de infracciones.*
>
> *3. Las personas que hayan denunciado o revelado públicamente información sobre infracciones de forma anónima pero que posteriormente hayan sido identificadas y sufran represalias seguirán, no obstante, teniendo derecho a protección en virtud del capítulo VI, siempre que cumplan las condiciones establecidas en el apartado 1.*

En este sentido, la posibilidad de presentar denuncias anónimas en los sistemas de información de denuncias internas ya había sido contemplada en nuestro ordenamiento jurídico en el artículo 24 de la LOPDGDD, en el que frente al criterio tradicionalmente sostenido por esta Agencia, en que se propugnaba el carácter confidencial y no anónimo de estos sistemas, se establece la posibilidad de que las denuncias sean comunicadas al sistema “incluso anónimamente”. Por consiguiente, debería mantenerse dicha posibilidad, al menos, en los supuestos contemplados en el citado artículo 24, en la medida en que la aplicación de la Directiva “no constituirá en ninguna circunstancia motivo para reducir el nivel de protección ya garantizado por los Estados miembros en los ámbitos regulados por la presente Directiva”, en virtud de la cláusula de no regresión contenida en su artículo 25.2.

A este respecto, el anteproyecto de ley prevé la posibilidad del anonimato en todos los canales internos, señalando en su artículo 7.3. que “Los canales internos deberán permitir la presentación y posterior tramitación

de comunicaciones anónimas", así como en el canal externo, en el cual, conforme al artículo 17, "La comunicación puede llevarse a cabo de forma anónima". Tal y como se justifica en la Exposición de Motivos "No hay mejor forma de proteger al que informa que garantizando su anonimato".

Por consiguiente, en los casos de que la comunicación se realice de forma anónima, si no es posible identificar a la persona informante, no sería de aplicación respecto de la misma la normativa de protección de datos personales, sin perjuicio de que deban adoptarse las medidas de garantía de la confidencialidad previstas en la norma. No obstante, teniendo en cuenta que la exclusión de la aplicación de la normativa de protección de datos requiere que la información personal no pueda asociarse a una persona física identificable, la simple omisión de los datos identificativos no implica que se trate de información anónima cuando la identidad se puede obtener de manera indirecta, como puede resultar, por ejemplo, en el caso de que la información comunicada únicamente la conozcan un número limitado de personas. Asimismo, la comunicación contendrá datos personales referidos a otros sujetos, como el presunto infractor o terceros que hayan tenido conocimiento, que sí tienen la consideración de datos personales, por lo que en ningún caso puede relajarse el nivel de protección de los datos personales del informante por el hecho de que la comunicación se realice de forma anónima.

Todo ello sin perjuicio de que deban adoptarse todas las medidas necesarias para garantizar dicho anonimato, de modo que los sistemas de denuncias se configuren de tal forma que, para la presentación anónima, no obtengan datos que permitan la identificación del informante, como puede ser la dirección IP o el número de teléfono, lo que debería reflejarse en el artículo 33 del anteproyecto, referido a la preservación de la identidad del informante y de las personas investigadas.

A este respecto, debe tenerse en cuenta, asimismo, la consideración de la voz como un dato personal, en la medida en que se refiere a una persona identificable, tal y como señaló el Tribunal Supremo en su sentencia 1771/2020 de 18 de junio de 2020: *"la grabación de la voz asociada a otros datos como el número de teléfono o su puesta a disposición de otras personas que pueden identificar a quien pertenece ha de considerarse un dato de carácter personal sujeto a la normativa de protección del tratamiento automatizado de los mismos".*

Por otro lado, también van a ser objeto de tratamiento los datos personales de las personas a las que se refiera la comunicación como presuntos infractores, a los que la Directiva se refiere como «persona afectada», entendiendo por tal, conforme a su artículo 5.10, la persona física o jurídica a la que se haga referencia en la denuncia o revelación pública como la persona a la que se atribuye la infracción o con la que se asocia la infracción", y que en el anteproyecto recibe la denominación de "persona investigada".

A este respecto, la Directiva prevé la adopción de medidas de protección en su artículo 22:

> *1. Los Estados miembros velarán, de conformidad con la Carta, por que las personas afectadas gocen plenamente de su derecho a la tutela judicial efectiva y a un juez imparcial, así como a la presunción de inocencia y al derecho de defensa, incluido el derecho a ser oídos y el derecho a acceder a su expediente.*
>
> *2. Las autoridades competentes velarán, de conformidad con el Derecho nacional, por que la identidad de las personas afectadas esté protegida mientras cualquier investigación desencadenada por la denuncia o la revelación pública esté en curso.*
>
> *3. Las normas establecidas en los artículos 12, 17 y 18 referidas a la protección de la identidad de los denunciantes se aplicarán también a la protección de la identidad de las personas afectadas.*

Asimismo, la información comunicada puede contener datos personales de terceras personas, como testigos o compañeros de trabajo, cuyos datos personales deben ser igualmente objeto de protección, tal y como resulta del Considerando 76 de la Directiva:

> *(76) Los Estados miembros deben velar por que las autoridades competentes dispongan de procedimientos de protección adecuados para el tratamiento de las denuncias y para la protección de los datos personales de quienes sean mencionados en la denuncia. Dichos procedimientos deben garantizar la protección de la identidad de cada denunciante, cada persona afectada y cada tercero que se mencione en la denuncia, por ejemplo, testigos o compañeros de trabajo, en todas las fases del procedimiento.*

Con objeto de dar cumplimiento a las previsiones de la Directiva, el artículo 33 del anteproyecto, anteriormente citado, regula la Preservación de la identidad del informante y de las personas investigadas:

> *1. Quien presente una comunicación o lleve a cabo una revelación pública tiene derecho a que su identidad no será revelada a terceras personas.*
>
> *2. Los sistemas internos de información, los canales externos y quienes reciban revelaciones públicas deberán contar con medidas técnicas y organizativas adecuadas para preservar la identidad y garantizar la confidencialidad de los datos correspondientes a las personas investigadas por la información suministrada, especialmente la identidad del informante en caso de que se hubiera identificado.*

3. La identidad del informante sólo podrá ser comunicada a la Autoridad judicial, al Ministerio Fiscal o a la autoridad administrativa competente en el marco de una investigación penal, disciplinaria o sancionadora.

Dicha regulación es conforme con la Directiva y la normativa sobre protección de datos personales, si bien debería modificarse el precepto para incluir expresamente, en su apartado 2, a cualquier tercero que se mencione en la denuncia, por ejemplo, testigos o compañeros de trabajo, tal y como prevé la Directiva, así como a la necesidad de incluir la protección del anonimato a la que anteriormente se ha hecho referencia.

Por otro lado, deben tenerse en cuenta las garantías específicas previstas en el apartado 3 del artículo 16 de la Directiva para el supuesto excepcional, contemplado en su apartado 2, de que se revele la identidad del denunciante:

2.Como excepción a lo dispuesto en el apartado 1, la identidad del denunciante y cualquier otra información prevista en el apartado 1 solo podrá revelarse cuando constituya una obligación necesaria y proporcionada impuesta por el Derecho de la Unión o nacional en el contexto de una investigación llevada a cabo por las autoridades nacionales o en el marco de un proceso judicial, en particular para salvaguardar el derecho de defensa de la persona afectada.
3. Las revelaciones hechas en virtud de la excepción prevista en el apartado 2 estará sujeta a salvaguardias adecuadas en virtud de las normas de la Unión y nacionales aplicables. En particular, se informará al denunciante antes de revelar su identidad, salvo que dicha información pudiera comprometer la investigación o el procedimiento judicial. Cuando la autoridad competente informe al denunciante, le remitirá una explicación escrita de los motivos de la revelación de los datos confidenciales en cuestión.

A este respecto, la redacción contenida en el apartado 3 del artículo 33 se considera demasiado genérica y no contiene, ni siquiera por referencia, las garantías que cita la Directiva. En este sentido, prevé la comunicación de la identidad a las autoridades que cita, pero no resuelve el problema del posible acceso de quienes sean parte en los procedimientos, singularmente, la revelación de la identidad del informante a la persona investigada como medio para salvaguardar su derecho de defensa. Por ello, y teniendo en cuenta que deberá atenderse a lo dispuesto en la legislación procesal penal y en la normativa sancionadora, sería necesario, al menos, la referencia a que la revelación de la identidad del denunciante en el transcurso de los correspondientes procedimientos solo procederá cuando sea necesario para salvaguardar el derecho de defensa de la persona afectada. En cuanto a las garantías, en el supuesto de la Autoridad Judicial o el Ministerio Fiscal, la misma resulta de la propia intervención de dichas autoridades y de la normativa

aplicable, lo que debería hacerse constar con la correspondiente remisión a su normativa específica.

En el caso de los procedimientos sancionadores, procede recordar el criterio que, respecto al acceso por parte del denunciado a los datos personales del denunciante, ha venido manteniendo esta Agencia desde el informe 142/2007, de 25 de julio de 2007:

> "Es decir, si el denunciante ha manifestado expresamente su deseo de confidencialidad o a juicio de la Unidad que deba resolver se entiende la necesidad de garantizar la identidad del denunciante en condiciones de confidencialidad, podrá denegarse el acceso solicitado mediante resolución debidamente motivada del órgano que deba resolver. Y en todo caso, por aplicación del apartado 3 del citado artículo 37, el solicitante deberá acreditar "un interés legítimo y directo" que justifique la cesión, a juicio de la Unidad responsable de resolver, habida cuenta que será una norma con rango de Ley (la propia Ley 30/1992) la que posibilite la cesión cuando concurran determinadas circunstancias".

Ante la falta de una regulación específica, dicho criterio se ha considerado vigente tras la entrada en vigor de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, tal y como se recoge en el Informe 74/2019.

No obstante, como consecuencia de la entrada en vigor de la Directiva (UE) 2019/1937, el mismo se ha invertido, ya que la regla general es la garantía de la confidencialidad, de modo que la revelación de la identidad del informante tiene carácter excepcional, siempre que resulte necesaria y proporcionada para salvaguardar el derecho de defensa de la persona investigada. Por ello, y ante la falta de una regulación específica de carácter general, debería incluirse la misma en el anteproyecto objeto de informe.

En este sentido, el propio anteproyecto contempla, respecto de instrucción del procedimiento por la Autoridad Independiente de Protección del Informante, que "En ningún caso se comunicará a los sujetos investigados la identidad del informante ni se dará acceso de la comunicación" y que "a fin de garantizar el derecho de defensa de la persona investigada, la misma tendrá acceso al expediente sin revelar información que pudiera identificar a la persona informante…", por lo que en estos casos el propio legislador estaría considerando que prevalece la protección del informante frente al derecho de defensa de la persona investigada (artículo 19.2, párrafo segundo y tercero). Sin embargo, nada se establece respecto de los supuestos en los que, conforme a lo previsto en el artículo 18, se acuerde remitir la comunicación a la autoridad, entidad u organismo que se considere competente para su tramitación o cuando afecte a los intereses de la Hacienda Pública o, en su caso, al Ministerio Fiscal si fueran indiciariamente constitutivos de delito.

Tampoco se establecen previsiones específicas respecto de los procedimientos disciplinarios o sancionadores que pueden tramitar las entidades del sector público y que se puedan iniciar como consecuencia de informaciones recibidas por el sistema interno de información.

Sin embargo, de la regulación del artículo 31 referida al derecho de información parece derivarse que la intención del legislador es impedir el conocimiento, en todo caso, de la identidad del informante o del que realice una revelación pública.

Por todo ello, se considera necesario modificar el artículo 33 para incluir las garantías específicas que permitirán, excepcionalmente, revelar la identidad del informante a la persona investigada, bien directamente, bien mediante remisión, en su caso, a la normativa legal que resulte de aplicación. O, en el supuesto de que se considere, conforme al principio de proporcionalidad y tal y como se ha realizado para los procedimientos tramitados por la autoridad independiente, que no procede en ningún caso revelar la identidad del denunciante a sujetos distintos de las propias autoridades contempladas en el precepto, debería reflejarse así en la propia norma, en aras de la seguridad jurídica y para evitar posteriores dudas interpretativas.

IV

La siguiente cuestión que se plantea es la relativa a la licitud del tratamiento, a la que el anteproyecto dedica el artículo 30:

Artículo 30. Licitud de los tratamientos de datos personales.
1. Se considerarán lícitos los tratamientos de datos personales necesarios para la aplicación de la presente ley.
2. El tratamiento de datos personales se entenderá lícito en base a lo que disponen los artículos 6.1.c) del Reglamento (UE) 2016/679 y 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 11 y 14, 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.
3. El tratamiento de datos personales en los supuestos de canales de comunicación externos se entenderá lícito en base a lo que disponen los artículos 6.1.c) del Reglamento (UE) 2016/679 y 8 de la Ley Orgánica 3/2018, de 5 de diciembre, y 11 de la Ley Orgánica 7/2021, de 26 de mayo.
4. El tratamiento de datos personales derivado de una revelación pública se presumirá amparado en lo dispuesto en el artículo 6.1.e) del

Reglamento (UE) 2016/679, y 11 de la Ley Orgánica 7/2021, de 26 de mayo.

Tal y como ya se ha avanzado, el Consejo de Estado en su Dictamen 757/2017, sobre el Anteproyecto de Ley Orgánica de Protección de Datos de Carácter Personal, consideró que el tratamiento de datos personales en los sistemas de denuncias internas quedaba legitimado por "la existencia de un interés público legitimador de estos tratamientos". Por consiguiente, con carácter general, estos tratamientos de datos personales se encuentran amparados por la letra e) del artículo 6.1 del RGPD: "el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento".

No obstante, tras la entrada en vigor de la Directiva (UE) 2019/1937, se ha establecido la obligación de establecimiento de canales de denuncia interna para determinadas entidades en su artículo 8, a las que el anteproyecto se refiere en el artículo 10, respecto del sector privado, y en el artículo 13, en cuanto al sector público. Asimismo, el artículo 11 de la Directiva (UE) 2019/1937 introduce una obligación de establecer canales de denuncia externa y de seguir las denuncias en su artículo 11, a la que el anteproyecto se refiere en su Título III, regulando el canal externo de comunicaciones de la Autoridad Independiente de Protección del Informante. Por consiguiente, en esto supuestos, el tratamiento encontraría su legitimación en la letra c) del artículo 6.1.del RGPD: el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento.

A este respecto, debe indicarse la trascendencia de que la legitimación venga determinada por uno u otro supuesto, en la medida en que el derecho de oposición previsto en el artículo 21 del RGPD, al que posteriormente nos referiremos, se reconoce respecto de los tratamientos basados en la letra e), pero no respecto de los amparados por la letra c).

Por otro lado, se cumple igualmente con el principio de reserva de ley derivado del artículo 53 de la Constitución, en los términos recogidos por el artículo 8 de la LOPDGDD.

En cuanto a la referencia que se incluye a la Ley Orgánica 7/2021, por la que se ha traspuesto la Directiva (UE) 2016/680, debe recordarse lo ya indicado respecto de su aplicación únicamente a los tratamientos de datos personales que se realicen por las autoridades competentes designadas en dicha ley, y a los específicos fines que la misma determina, no siendo de aplicación a los sujetos que tienen una obligación de colaborar con dichas autoridades, cuyos tratamientos se rigen por el RGPD.

No obstante, cuando se trate de categorías especiales de datos, será requisito indispensable que, con carácter previo, concurra alguna de las causas que levanten la prohibición de su tratamiento conforme al artículo 9.2. del RGPD. A este respecto, el anteproyecto no contiene mención alguna respecto del posible tratamiento de estos datos, debiendo tenerse en cuenta que en las informaciones que se reciban puede contenerse este tipo de información.

Esta Agencia considera que, con carácter general, el tratamiento de las categorías especiales de datos a las que se refiere el artículo 9.1. del RGPD no resultará necesario para la gestión de las comunicaciones recibidas y la tramitación de los correspondientes procedimientos, por lo que debería recogerse expresamente en el anteproyecto que si la información recibida contuviera datos personales incluidos dentro de las categorías especiales de datos, se procederá a su inmediata supresión, sin que se proceda al registro y tratamiento de los mismos.

No obstante, si previo el análisis de riesgos al que nos referíamos en el primer apartado del presente informe, se considerara necesario que en determinados supuestos se trataran categorías especiales de datos personales, su tratamiento podría realizarse conforme a lo previsto en la letra g) del artículo 9.2. del RGPD: 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 este caso, debería recogerse expresamente en el anteproyecto dicha posibilidad, identificando qué tipos de datos personales incluidos en las categorías especiales de datos podrían ser objeto de tratamiento, y limitarlos a los estrictamente necesarios, previendo su supresión inmediata en cuanto no sean necesarios y estableciendo, en su caso, las garantías adicionales que resulten del correspondiente análisis de riesgos para la adecuada protección de los intereses y derechos fundamentales del interesado.

V

Una vez determinada la licitud del tratamiento, deben establecerse en la norma las garantías específicas que permitan cumplir con el resto de principios de protección de datos 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»).

En cuanto al principio de limitación de la finalidad, al tratarse de tratamientos amparados en las letras c) y e) del RGPD, la finalidad del tratamiento deberá quedar determinada en la propia norma que legitima el tratamiento.

A este respecto, dicha finalidad resulta de lo previsto en los artículos 1 (finalidad de la ley) 2 (ámbito material de aplicación) y 3 (ámbito personal de aplicación) del anteproyecto, que no se limita a la mera trasposición de la directiva sino que además pretende un amplio de protección del informante más amplio en todos los supuestos que se identifican en el artículo 2.

A este respecto, haciendo uso de la facultad prevista en el apartado 2 del artículo 2 de la directiva, se incluyen en el ámbito material de aplicación material del artículo 2 del anteproyecto en su apartado b):

Acciones u omisiones que puedan ser constitutivas de infracción penal o administrativa grave o muy grave o cualquier vulneración del resto del ordenamiento jurídico siempre que, en cualquiera de los casos, afecten o menoscaben directamente el interés general, y no cuenten con una regulación específica. En todo caso, se entenderá afectado el interés general cuando la acción u omisión de que se trate implique quebranto económico para la Hacienda Pública.

De este modo, el ámbito de aplicación parece limitarse, en un primer momento a los supuestos de infracción penal o administrativa grave o muy grave siempre que afecte o menoscabe directamente el interés general, para posteriormente ampliarlo a cualquier vulneración del resto del ordenamiento jurídico que igualmente afecte o menoscabe directamente el interés general, sin hacer referencia en este caso a su posible gravedad.

Se trata, en opinión de esta Agencia, de una previsión excesivamente genérica que supone la aplicación de un concepto jurídico indeterminado y que, dadas las implicaciones que la aplicación de la normativa proyectada tiene respecto de la protección de los datos personales, incluidos los de las personas investigadas, y las limitaciones que a dicho derecho se establecen, por aplicación del principio de limitación de la finalidad debería buscarse una redacción más precisa que identificara las posibles vulneraciones que afecten al interés general, o los ámbitos en las que las mismas pueden producirse, teniendo en cuenta, además su posible gravedad.

Por otro lado, la aplicación de los restantes principios de protección de datos en los sistemas de información internos requiere que se establezcan garantías específicas, a las cuales se refiere el artículo 32 del anteproyecto, en el que se han incluido las que están previstas en el artículo 24 de la LOPDGDD:

Artículo 32. Tratamiento de datos personales en los Sistemas internos de información.

1. El acceso a los datos personales contenidos en los Sistemas internos de información quedará limitado, dentro del ámbito de sus competencias y funciones, exclusivamente a:

a) El responsable del Sistema y a quien lo gestione directamente.

b) El responsable de recursos humanos, sólo cuando pudiera proceder la adopción de medidas disciplinarias contra un trabajador. En el caso de los empleados públicos, el órgano competente para la tramitación del mismo.

c) El responsable de los servicios jurídicos de la entidad u organismo, si procediera la adopción de medidas legales en relación con los hechos relatados en la comunicación.

d) Los encargados del tratamiento que eventualmente se designen.

e) El Delegado de Protección de Datos.

2. Será lícito el tratamiento de los datos por otras personas, o incluso su comunicación a terceros, cuando resulte necesario para la tramitación de los procedimientos sancionadores o penales que, en su caso, procedan.

3. Los datos que sean objeto de tratamiento podrán conservarse en el sistema de informaciones únicamente durante el tiempo imprescindible para decidir sobre la procedencia de iniciar una investigación sobre los hechos informados. 47

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.

5. Los empleados y terceros deberán ser informados acerca de la existencia de los sistemas de información a que se refiere el presente artículo.

La primera cuestión que se plantea es el acceso a los datos personales contenidos en los Sistemas, que debe limitarse a aquellos que tengan la necesidad de conocer dichos datos personales en función de las competencias que tengan atribuidas. En este sentido, el artículo 24.2 de la LOPDGDD prevé, respecto de los establecidos por entidades privadas, que “quedará limitado exclusivamente a quienes, incardinados o no en el seno de la entidad, desarrollen las funciones de control interno y de cumplimiento, o a los encargados del tratamiento que eventualmente se designen a tal efecto. […] solo cuando pudiera proceder la adopción de medidas disciplinarias contra un trabajador, dicho acceso se permitirá al personal con funciones de gestión y control de recursos humanos”.

El texto proyectado procede a una enumeración de las personas que podrán acceder a los datos personales, que esta Agencia considera que se ajusta a la anterior previsión, si bien sería conveniente justificar en la MAIN las razones que llevan a esa inclusión. En todo caso, destaca la referencia al DPD, al que posteriormente nos referiremos, en el que la posibilidad de acceder a los datos personales para el ejercicio de sus funciones deriva del propio RGPD.

Por otro lado, se hace referencia, igualmente, a la posible comunicación de los datos cuando resulte necesario para la tramitación de los procedimientos sancionadores o penales que, en su caso, procedan, previsión que debe ponerse en conexión con las disposiciones para la preservación de la identidad del informante contenidas en el artículo 33, al que ya nos hemos referido.

Asimismo, se incluye en el precepto la normativa recogida en el artículo 24.4 de la LOPDGDD referida a la limitación del plazo de conservación de los

datos personales en los Sistemas. Estas obligaciones son independientes de la existencia del libro-registro a que se refiere el artículo 26, por lo que deben cumplirse en todo caso, independientemente de los datos personales que se hayan podido reflejar en el libro-registro, que está sometido a garantías específicas, destacando singularmente que al mismo solo pueda accederse en virtud de auto judicial.

Esta Agencia valora muy positivamente la regulación que del registro previsto en el artículo 18 de la directiva se realiza en el anteproyecto, introduciendo dicha intervención judicial como garantía específica que el acceso a los datos reflejados en el mismo solo pueda realizarse "a petición razonada de la Autoridad judicial competente, mediante auto, y en el marco de un procedimiento judicial y bajo la tutela de aquélla, podrá accederse total o parcialmente al contenido del referido registro". De este modo, se permite compatibilizar la necesaria supresión de los datos personales en los sistemas internos de información, sometidos a un régimen de acceso más amplio, una vez transcurridos los plazos que se recogen en el artículo 32 del anteproyecto, limitados al tiempo imprescindible para decidir sobre la procedencia de iniciar una investigación, con un plazo máximo de tres meses, con la obligación de llevar el citado registro, en el que se establece un plazo de conservación más amplio que puede alcanzar los diez años.

Por otro lado, otro de los principios fundamentales en materia de protección de datos personales es el de minimización de datos, de modo que los datos que se incluyan en los sistemas sean solo los necesarios, adecuados y pertinentes para la finalidad pretendida, debiendo velar por ello los correspondientes responsables. Sin perjuicio de ser una obligación que viene directamente impuesta por el RGPD, se considera conveniente que el artículo 32 se incluya una referencia expresa, señalando que en ningún caso serán objeto de tratamiento los datos personales que no sean necesarios para el conocimiento e investigación de las acciones u omisiones a las que se refiere el artículo 2, procediéndose, en su caso, a su inmediata supresión. Asimismo, 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.

Mayores problemas plantea el principio de exactitud de los datos, ya que en muchas ocasiones la información remitida puede responder a meras sospechas, razón por la cual tanto la directiva como el anteproyecto prevén, para poder gozar de la protección que otorgan, que "tengan motivos razonables para pensar que la información referida es veraz en el momento de la comunicación o revelación, aun cuando no aporten pruebas concluyentes". Por ello, si se acreditara que la información facilitada o parte de ella no es veraz, deberá procederse a su inmediata supresión desde el momento en que se tenga constancia de dicha circunstancia, lo que también debería recogerse en el artículo 32.

La inclusión de dichas garantías deriva de lo previsto en la propia Directiva (UE) 2019/1937, cuyo apartado 2 del artículo 17 contiene una previsión específica para garantizar dichos principios, que debe ser oportunamente incorporada al ordenamiento jurídico interno: *"No se recopilarán datos personales cuya pertinencia no resulte manifiesta para tratar una denuncia específica o, si se recopilan por accidente, se eliminarán sin dilación indebida".*

En cuanto al principio de integridad y confidencialidad, así como al de responsabilidad proactiva, corresponde al responsable y, en su caso, al encargado, adoptar todas las medidas necesarias para garantizar la protección de los derechos y libertades de los afectados por el tratamiento de sus datos personales, incluidas las correspondientes medidas de seguridad de los datos, reforzadas, entre otros aspecto, respecto a la necesaria confidencialidad y, singularmente, la revelación de la identidad del informante. En este ámbito, adquieren especial relevancia las medidas de responsabilidad proactiva contenidas en el RGPD, y que deberán ser tenidas en cuenta en el diseño e implementación de los Sistemas de información, tanto internos como externos, incluido el análisis de riesgos el artículo 24, la necesidad de preservar la privacidad desde el diseño y por defecto del artículo 25, la realización de una Evaluación de impacto en la protección de datos del artículo 35 y las medidas de seguridad del artículo 32, todos ellos del RGPD.

Desde esta perspectiva, destaca la designación obligatoria de un delegado de protección de datos, prevista en el artículo 34 del anteproyecto, por todas aquellas entidades obligadas a disponer de un sistema interno de comunicaciones y por las autoridades independientes, lo que sin duda constituye una garantía adicional para la protección del derecho fundamental.

Por otro lado, el RGPD exige a los responsables de un tratamiento de datos personales tener en cuenta la naturaleza del tratamiento, su contexto, su ámbito y alcance, y sus fines con el fin de determinar las posibles consecuencias negativas o riesgos que podría derivar del tratamiento de sus datos personales. En este sentido es preciso tener en cuenta la necesidad de realizar un detallado análisis de toda la información que podría contener un sistema de información destinado a dar respuesta a las obligaciones que exige la normativa aplicable, tanto sectorial como de protección de datos personales, información que permitirá de manera indirecta o directa la identificación de personas físicas, ya sean los informantes o terceros.

Para llevar a cabo el análisis de estos identificadores la normativa de protección de datos personales, en particular el RGPD, pone en manos de los responsables de un tratamiento de datos personales la herramienta de evaluación de impacto en protección de datos personales que puede utilizarse

en el desarrollo de la propia normativa (Artículo 35.10 RGPD) o con carácter previo a la puesta en marcha de un tratamiento de datos personales. Entendiendo que tanto por su naturaleza como por el contexto en el que se tratarán los datos personales, hablamos de un tratamiento de datos de alto riesgo para los derechos y libertades de las personas físicas y, por tanto, la herramienta de evaluación de impacto en protección de datos personales se convierte en una obligación de los responsables para proteger los derechos y libertades de las personas físicas cuyos datos serán tratados mediante informaciones o identificadores directos (nombres, apellidos, cargo, DNI, etc.) o indirectos (IP, hora de conexión, ID del dispositivo, MAC, cookies, fingerprinting, etc.), será de obligado cumplimiento para el responsable, dar respuesta a lo previsto en el artículo 35.7 del RGPD, realizando, en el contexto de las actividades de una evaluación de impacto en protección de datos las siguientes actuaciones:

a) Una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, en la que se realizará el análisis de los datos e identificadores personales que se incluirán en el sistema de información, que hagan identificables a las personas así como las operaciones de tratamiento que podrían realizarse

b) Una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con relación a los datos o identificadores personales que se hubieran identificado en la descripción sistemática del mismo atendiendo al principio de necesidad y proporcionalidad de las mismas con relación a los fines para los que fueran a ser recogidos

c) La identificación de los riesgos que las operaciones de tratamiento podrían implicar para los interesados, incluyendo las medidas previstas para eliminar los riesgos para las personas físicas derivados de dichas operaciones de tratamiento que hubieran sido identificadas en la descripción sistemática del tratamiento, estableciendo medidas y garantías, entre las que, de acuerdo a la naturaleza del tratamiento, cobrarían especial importancia las orientadas a dar cumplimiento al principio de minimización (Artículo 25.2 del RGPD) así como las medidas de seguridad entre las que serían especialmente relevantes las destinadas a dar cumplimiento a la adecuada seudonimización y cifrado de los datos, cuando fuera necesario, atendiendo a las obligaciones que establece el artículo 32.1.a. Todo ello sin perjuicio del resto de obligaciones derivadas de la normativa de protección de datos (RGPD y LOPDGDD) así como de la normativa sectorial que también le fuera de aplicación al tratamiento de los datos que pudiera realizarse en el ámbito de aplicación de la presente norma como, por ejemplo, la obligación de incluir dicha actividad de tratamiento en su Registro de Actividad de Tratamiento y en su inventario de actividad de tratamiento.

En este sentido y tal como se define en el documento relativo a las “Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del RGPD”, del Comité Europeo de Protección de Datos,

adoptadas el 4 de abril de 2017, se debe entender que “Una EIPD es un proceso concebido para describir el tratamiento, evaluar su necesidad y proporcionalidad y ayudar a gestionar los riesgos para los derechos y libertades de las personas físicas derivados del tratamiento de datos personales evaluándolos y determinando las medidas para abordarlos. Las EIPD son instrumentos importantes para la rendición de cuentas, ya que ayudan a los responsables no solo a cumplir los requisitos del RGPD, sino también a demostrar que se han tomado medidas adecuadas para garantizar el cumplimiento del Reglamento (véase asimismo el artículo 24)5. En otras palabras, una EIPD es un proceso utilizado para reforzar y demostrar el cumplimiento.”

En consecuencia con la naturaleza, el contexto, el ámbito o alcance y los fines de cualquiera de las operaciones de tratamiento que pudieran realizarse en el ámbito de las actividades de tratamiento derivadas de la aplicación de la presente norma, a tenor del potencial de riesgo de las mismas para los derechos y libertades de los interesados, la EIPD es una actividad obligada para cualquier responsable.

Por ello, con el fin de reforzar las garantías, debe incluirse, asimismo, la obligación de realizar una Evaluación de impacto, que el artículo 35 del RGPD prevé para los supuestos en los que “sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas”.

Por otro lado, debería recogerse la obligación del personal de las autoridades independientes que vaya a recibir y tramitar las comunicaciones, de recibir formación sobre las normas aplicables en materia de protección de datos, conforme a lo previsto en el artículo 12.5 y el Considerando 74 de la Directiva (UE) 2019/1937. Asimismo, podría extenderse dicha obligación al personal que vaya a gestionar los sistemas internos de información.

VI

Para concluir, debe hacerse referencia a los derechos de los afectados por el tratamiento de sus datos personales, comenzando con el deber de información previsto en los artículos 12 a 14 del RGPD, al cual se refiere el artículo 25, al referirse a la información sobre los canales internos y externos de información, que incluirá “d) El régimen de confidencialidad aplicable a las comunicaciones, y en particular, la información sobre el tratamiento de los datos personales de conformidad con lo dispuesto en el Reglamento (UE) 2016/679, la Ley Orgánica 3/2018, y el título VI”, el artículo 32.5. que recoge la

obligación de informar a empleados y terceros de la existencia de los sistemas internos de información y, específicamente, el artículo 31:

Artículo 31. Información a los interesados y ejercicio de derechos.

1. Cuando se obtengan directamente de los interesados sus datos personales se les facilitará la información a que se refieren los artículos 13 del Reglamento (UE) 2016/679 y 11 de la Ley Orgánica 3/2018, de 5 de diciembre.

A los informantes y a quienes lleven a cabo una revelación pública se les informará, además, de forma expresa, de que su identidad será en todo caso reservada, que no se comunicará a las personas a las que se refieren los hechos relatados ni a terceros.

Además, a quienes realicen la comunicación a través de canales internos se les informará, de forma clara y fácilmente accesible, sobre los canales externos de información ante las autoridades competentes y, en su caso, ante las instituciones, órganos u organismos de la Unión Europea.

A este respecto, debe indicarse que la información a la que se refiere el párrafo tercero no guarda relación con la protección de datos personales, por lo que debería ubicarse en otro precepto del propio texto, como el citado artículo 25, estando ya previsto en el artículo 8.

Por otro lado, dicho apartado se refiere únicamente a la información a los interesados cuando se obtiene los datos directamente de ellos, sin embargo, no resuelve la cuestión relativa al cumplimiento del deber de información previsto en el artículo 14 del RGPD, cuando los datos no se obtienen directamente de los interesados, como es el caso de la persona a la que se refieran los hechos o terceros a los que la información se refiera como, por ejemplo, compañeros o testigos.

A este respecto, el artículo 8, incluye entre los principios del procedimiento de gestión de comunicaciones, en apartado 2 letra d: *"Establecimiento del derecho del informante (sic) a que se le informe de las acciones u omisiones que se le atribuyen, y a ser oído en cualquier momento. Dicha comunicación tendrá lugar en el tiempo y forma que se considere adecuado para garantizar el buen fin de la investigación"*.

En dicho precepto se observa una errata, por lo que debe modificarse el citado artículo 8.2.d) en cuanto no se está refiriendo al informante sino a la persona a la que se refiere la información.

En cuanto al canal externo, el artículo 19.2. prevé la posibilidad de retrasar la información para no perjudicar la investigación: *"Se garantizará que la persona investigada por la comunicación tenga noticia de la misma, así como de los hechos relatados de manera sucinta. Adicionalmente se le informará del derecho que tiene a presentar alegaciones por escrito y del tratamiento de sus datos personales. No obstante, esta información podrá*

efectuarse en el trámite de audiencia si se considerara que su aportación con anterioridad pudiera facilitar la ocultación, destrucción o alteración de las pruebas”.

La necesidad de limitar los derechos de los afectados por el tratamiento de los datos personales aparece expresamente prevista en los Considerandos 84 y 85 de la Directiva (UE) 2019/1937:

> *(84) Los procedimientos establecidos en la presente Directiva y relacionados con el seguimiento de denuncias de infracciones del Derecho de la Unión en sus ámbitos de aplicación contribuyen a un objetivo importante de interés público general de la Unión y de los Estados miembros, en el sentido del artículo 23, apartado 1, letra e), del Reglamento (UE) 2016/679, ya que su objetivo es mejorar la ejecución del Derecho y las políticas de la Unión en determinados ámbitos en los cuales el incumplimiento puede provocar graves perjuicios para el interés público. Una protección efectiva de la confidencialidad de la identidad de los denunciantes resulta necesaria a fin de proteger los derechos y libertades de los demás, en particular los de los propios denunciantes, tal como establece el artículo 23, apartado 1, letra i), del Reglamento (UE) 2016/679. Los Estados miembros deben velar por que la presente Directiva sea eficaz, incluso, cuando sea necesario, restringiendo mediante medidas legislativas el ejercicio de determinados derechos de protección de datos de las personas afectadas en consonancia con el artículo 23, apartado 1, letras e) e i), y el artículo 23, apartado 2, del Reglamento (UE) 2016/679, en la medida y durante el tiempo que sea necesario a fin de evitar y abordar los intentos de obstaculizar las denuncias o de impedir, frustrar o ralentizar su seguimiento, en particular las investigaciones, o los intentos de averiguar la identidad del denunciante.*
>
> *(85) Una protección efectiva de la confidencialidad de la identidad del denunciante resulta igualmente necesaria a fin de proteger los derechos y libertades de los demás, en particular los del propio denunciante, cuando la denuncia la tratan las autoridades tal como se definen en el artículo 3, punto 7, de la Directiva (UE) 2016/680. Los Estados miembros deben velar que la presente Directiva sea eficaz, incluso, cuando sea necesario, restringiendo mediante medidas legislativas el ejercicio de determinados derechos de protección de datos de las personas afectadas en consonancia con el artículo 13, apartado 3, letras a) y e), el artículo 15, apartado 1, letras a) y e), el artículo 16, apartado 4, letras a) y e), y el artículo 31, apartado 5, de la Directiva (UE) 2016/680, en la medida y durante el tiempo que sea necesario a fin de evitar y abordar los intentos de obstaculizar las denuncias o de impedir, frustrar o ralentizar su seguimiento, en particular*

las investigaciones, o los intentos de averiguar la identidad del denunciante.

Por consiguiente, sin perjuicio de las menciones específicas contenidas en casos particulares en el texto y a las que se ha hecho referencia, debería recogerse expresamente en el artículo 31 del anteproyecto, la forma en que se procederá al cumplimiento del deber de información respecto de la persona a la que se refiere la información y aquellos otros a los que se cita en la misma y que puedan tener participación en el procedimiento, como pueden ser los testigos, pudiendo limitarse el cumplimiento de dicho deber al momento en el que no se perjudique el buen fin de la investigación, respecto del primero, y al momento en el que vayan a intervenir en el procedimiento, respecto de los segundos.

Por otro lado, como limitación específica que afecta no solo al derecho de información sino también al de acceso, se prevé que *"La persona a la que se refieran los hechos relatados no será en ningún caso informada de la identidad del informante o de quien haya llevado a cabo la revelación pública"*.

Por otro lado, el artículo 31, en su apartado 4 señala que *"En caso de que la persona a la que se refieran los hechos relatados en la comunicación o a la que se refiera la revelación pública ejerciese el derecho de oposición se presumirá que, salvo prueba en contrario, existen motivos legítimos imperiosos que legitiman el tratamiento de sus datos personales".*

A este respecto, tal y como se ha indicado al analizar la licitud del tratamiento, el derecho de oposición únicamente procede respecto de los supuestos en que el tratamiento se legitima en la letra e) del artículo 6.1. del RGPD, pero no respecto de los supuestos en los que el mismo se ampara en la letra c) del mismo. Por otro lado, debe recordarse que existen supuestos en nuestro ordenamiento jurídico en los que, por razones de interés público, se excluye directamente el derecho de oposición, como ocurre en el artículo 28.2. de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas: *"No cabrá la oposición cuando la aportación del documento se exigiera en el marco del ejercicio de potestades sancionadoras o de inspección".*

VII

Por último, la disposición final cuarta modifica el artículo 24 de la LOPDGDD para adecuarla a la nueva regulación, suprimiendo la regulación específica que contenía y remitiendo a lo previsto en la nueva normativa, lo que se considera adecuado en aras de la necesaria seguridad jurídica.