La protección de datos de carácter personal en el marco de los procedimientos de información sobre infracciones normativas

Leonor Rams Ramos
Profesora titular de Derecho Administrativo de la Universidad Rey Juan Carlos. Delegada de protección de datos

SUMARIO. 1. Introducción. 2. La protección de datos personales en los mecanismos de información de la Ley 2/2023. 2.1. La preocupación del legislador por garantizar el cumplimiento del principio de licitud del tratamiento: la búsqueda de bases de legitimación en función de la vía de denuncia utilizada. 2.2. El cumplimiento del principio de responsabilidad proactiva. **3. Protección de datos desde el diseño y por defecto en la implementación de los sistemas internos de información y en los procedimientos de gestión de los mismos.** 3.1. La determinación de los responsables y encargados de tratamiento en el marco de los sistemas internos de información y la aplicación del principio de confidencialidad en la limitación de las personas con acceso al Sistema. 3.2. Finalidad, integridad y transparencia. 3.3. Tratamiento de los datos personales en el procedimiento de gestión de la información. **4. Bibliografía.**

1. Introducción

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, y que traspone la Directiva 2019/1937 del Parlamento Europeo y del Consejo, relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión, plantea numerosos desafíos desde el punto de

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 38
ISBN: 978-84-125912-4-8

vista del derecho a la protección de los datos de carácter personal, no solo por cuanto, justamente, esa "protección" que se debe prestar a los denunciantes tiene su base en la necesaria protección de su identidad y de otros datos personales suyos, sino también, muy especialmente, porque su aplicación implica la creación de sistemas y procedimientos de gestión de la información que comunican estos denunciantes, que implican tratamientos de datos personales —no solo del propio informante, sino también de otras personas— que deben implantarse y gestionarse desde el respeto a la normativa de protección de datos, en especial 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 y por el que se deroga la Directiva 95/46/CE (en adelante, RGPD), y la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos de carácter personal y garantía de los derechos digitales (en adelante, LOPDGDD), que ha sido modificada, como veremos, por la propia Ley 2/2023, para reforzar la base de legitimación de estos tratamientos.

Toda la ley, por tanto, alude a la necesaria protección de datos personales, desde una doble perspectiva: como propio objeto de la norma, pues la finalidad declarada de la misma es la garantía de la protección de los informantes —a través de la confidencialidad en el tratamiento de sus datos personales, en particular por lo que se refiere a su identidad—, pero también desde la perspectiva de que los mecanismos que se implantan para su protección —los sistemas de información interno, externo y de revelación pública— deben respetar la normativa de protección de datos personales y, en particular, los principios que rigen el tratamiento de los datos, según establece el artículo 5 del RGPD, así como la LOPDGDD y, en su caso, 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 (en adelante, LO 7/2021).

Podría darse cabida aquí a un sinfín de cuestiones, pero en este estudio nos vamos a centrar, por razones lógicas de espacio, en un aspecto fundamental: la garantía del cumplimiento de la normativa de protección de datos personales en los procedimientos de información que se activen, consecuencia de la actuación de los denunciantes. Para ello, partiremos de analizar el encaje de los tratamientos de datos personales que implica la implantación de los mecanismos de denuncias con la normativa de protección de datos, muy particularmente en relación con el cumplimiento de los principios relativos al tratamiento que regula el RGPD, para, desde ahí,

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 38
ISBN: 978-84-125912-4-8

estudiar las medidas que la Ley 2/2023 establece no solo en cuanto a la garantía del derecho a la protección de datos personales en el marco de los procedimientos de información, sino también, de manera esencial, en los canales de gestión de las informaciones que los sujetos obligados por la ley deben implementar.

2. La protección de datos personales en los mecanismos de información de la Ley 2/2023

La Ley 2/2023 establece varios mecanismos para canalizar las denuncias —informaciones, según nuestra ley[1]- que se refieran a incumplimientos del derecho de la Unión Europea, así como de determinadas normas jurídicas nacionales, que no tengan sus propios mecanismos de denuncia establecidos.

Todos ellos: el Sistema interno de información —al que están obligadas un gran número de entidades del sector privado y la mayoría de las entidades del sector público—, el Canal externo de información —que debe implantar la Autoridad Independiente de Protección del Denunciante, A.A.I., y, en su caso, las autoridades que al efecto creen las comunidades autónomas—, así como las revelaciones públicas hechas por los denunciantes, incluso si las mismas son anónimas —cosa que permite la normativa mencionada—, implican tratamientos de datos personales, por lo que deben cumplir con las normas reguladoras de la protección de datos de carácter personal, en particular, como hemos visto ya, el RGPD y la LOPDGDD.

Desde esta perspectiva, resulta reseñable la preocupación que muestra el legislador, explicitada tanto en el preámbulo como en el propio texto articulado de la norma, por justificar el cumplimiento de la normativa de protección de datos[2], si bien está claro que es un reflejo de la preocupación

1. El preámbulo de la ley explicita la opción de no utilizar los términos de la Directiva: denunciantes, alertadores, etc., optando por el término más neutro de "informadores" y canales de información. No obstante, esto genera a veces cierta confusión, e incluso la propia norma sigue hablando de "denunciantes" (artículo 4), por lo que no se acaba de entender esta elección. Por razones de claridad, en este trabajo optamos por utilizar también este término, dado que tiene explícita acogida en la norma, no sin criticar —o denunciar— la falta de coherencia que muestra el legislador en este caso.

2. Aunque esto pueda parecer una obviedad, no está de más recordar que son numerosísimas las normas que se aprueban en nuestro ordenamiento jurídico que, pese a implicar tratamiento de datos personales, obvian esta cuestión y no contienen ninguna referencia al respecto. Véase, por ejemplo, la recientemente aprobada Ley Orgánica 2/2023, del Sistema Universitario, pese a que la anterior Ley Orgánica de Universidades, en su modificación de 2007, incluyó una base de legitimación para el tratamiento de los datos de los estudiantes. En la mayoría de los casos, las leyes se limitan a establecer una genérica referencia al cumplimiento del RGPD y de la LOPDGDD para los tratamientos de datos personales.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 38
ISBN: 978-84-125912-4-8

que la Directiva 2019/1937 había mostrado por esta cuestión, estableciendo garantías específicas al respecto[3].

Sin embargo, la doctrina[4], como ya hiciera la Agencia Española de Protección de Datos (en adelante, AEPD)[5], han mostrado su preocupación respecto del carácter meramente formal y poco específico, en ocasiones, en relación con esta regulación, que parece incidir de manera muy insistente en la necesidad de justificar la licitud de los tratamientos —sobre lo que vuelve una y otra vez, como veremos, tanto en el preámbulo como en el articulado—, pero sin profundizar de manera excesiva respecto de su plena justificación.

En este sentido, la Ley 2/2023 dedica su título VI a la protección de datos personales, con carácter trasversal y de aplicación tanto a los sistemas internos de información como al canal externo, e incluso a la revelación pública, prestando efectivamente especial atención a la cuestión de la licitud de los tratamientos en cada uno de estos supuestos.

El legislador, como no podría ser de otra forma, comienza indicando en este título VI que los tratamientos personales que se deriven de la aplicación de la norma se rigen por la normativa de protección de datos, aludiendo de manera específica al RGPD, a la LOPDGDD y a la LO 7/2021 y lo establecido en el propio título VI de la ley (artículo 29). Y, considerando el carácter central que tiene en la normativa de protección de datos el artículo 5 del RGPD, que regula los principios por los que se rigen los tratamientos, gran parte de este título VI se centra en la aplicación de dichos principios en el ámbito que nos ocupa, pero haciendo en algunos casos alusiones meramente formales o, en ocasiones, fragmentadas de los mismos[6].

3. Sobre esta cuestión, véase el trabajo de Piñar Mañas (2020: 101).

4. Véase, entre otros, Fernández Salmerón (2023: 197).

5. Informe del Gabinete Jurídico de la AEPD 0020/2022, al Anteproyecto de la Ley reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción.

6. Valga, como ejemplo clarificador de esta cuestión, que el artículo 29, después de enunciar la aplicación de la normativa de protección de datos, establece a continuación que "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". Se está aludiendo aquí, no hay duda, a los principios de lealtad y minimización que establece el RGPD, pero la sistemática utilizada por la norma en este sentido no parece la más adecuada, por cuanto este principio de minimización, en todo caso, debe completarse con otros —exactitud, limitación temporal, confidencialidad, etc.— de igual relevancia, y además al mismo también se alude en relación con el tratamiento de datos en el Sistema interno de información, que se contiene en el artículo 32 de la ley.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 38
ISBN: 978-84-125912-4-8

2.1. La preocupación del legislador por garantizar el cumplimiento del principio de licitud del tratamiento: la búsqueda de bases de legitimación en función de la vía de denuncia utilizada

De manera reiterativa, como señalábamos, el legislador muestra una gran preocupación por cumplir con el principio de licitud, por lo que dedica el artículo 30 de la Ley 2/2023 a explicitar las bases de legitimación para el tratamiento de los datos personales en los distintos supuestos que implica la norma.

De entrada, el artículo 30.1 establece la legitimación en la propia ley implícitamente aludiendo a la base de legitimación del artículo 6.1.c) del RGPD, lo cual se refuerza, además, mediante la reforma del artículo 24 de la LOPDGDD por la disposición final séptima[7], y sin embargo pivota después entre esta base de legitimación legal y la establecida por el artículo 6.1.e) del RGPD relativa al cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento, en función de la vía de comunicación de que se trate.

Así, para los supuestos de comunicación a través de los sistemas de información internos, se alude a la base de legitimación establecida por el artículo 6.1.c) del RGPD, completada en su caso con las disposiciones de los artículos 8 de la LOPDGDD y 11 de la LO 7/2021 —ambos preceptos vienen referenciados en el preámbulo—, y que luego además se refuerza, como acabamos de ver, con la reforma del artículo 24 de la LOPDGDD, en una suerte de retroalimentación normativa de licitud.

Sin embargo, en esa aparentemente excesiva preocupación del legislador por dotar de cobertura legal a todos los posibles tratamientos de datos derivados de las denuncias, el artículo 30.2 establece que cuando no sea

No tiene sentido, en todo caso, la inclusión reiterativa del principio de minimización, por cuanto más adelante se habla de supresión de nuevo, en el mencionado artículo 32; ni tampoco que se hable de recopilación de datos "por accidente".

7. Resulta de utilidad mencionar, de manera específica, el nuevo artículo 24 de la LOPDGDD, que ya establecía de manera específica la licitud de los sistemas de denuncias internas en el ámbito del sector privado, y que ahora queda de la siguiente manera:

"Artículo 24. Tratamiento de datos para la protección de las personas que informen sobre infracciones normativas.

Serán lícitos los tratamientos de datos personales necesarios para garantizar la protección de las personas que informen sobre infracciones normativas.

Dichos tratamientos se regirán por lo dispuesto en el Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, en esta ley orgánica y en la Ley reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción".

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 38
ISBN: 978-84-125912-4-8

obligatorio disponer de un Sistema interno de información "el tratamiento se presumirá amparado en el artículo 6.1.e) del citado reglamento"[8].

Lo mismo ocurre cuando en el apartado 4 del citado artículo 30 de la ley se legitima el tratamiento de datos personales derivado de una revelación pública en el mismo artículo 6.1.e) y en el artículo 11 de la LO 7/2021[9].

Resulta algo extraño que, si lo que el legislador pretendía era justamente que estos preceptos sirvieran de atribución competencial tanto a las entidades privadas no obligadas a tener canales de denuncia como en el caso de las revelaciones públicas, no se haya remitido a la base de legitimación del artículo 6.1.c) del RGPD, mil veces reforzada en la propia ley y con la modificación del artículo 24 de la LOPDGDD, sino que se acuda a una base de legitimación claramente acotada, tanto por el derecho de la Unión Europea como por la LOPDGDD, a un ámbito de ejercicio de competencias públicas establecidas por ley[10].

8. Debemos tener en cuenta que la ley determina las entidades obligadas a disponer de un Sistema interno de información en sus artículos 10 —referido a las entidades obligadas del sector privado— y 13 —entidades obligadas en el sector público, incorporando "a los efectos de la ley" básicamente todas las entidades que engrosan el sector público según el artículo 2 de la Ley 40/2015, de Régimen Jurídico del Sector Público—. Es decir, que cuando pensamos en entidades que puedan establecer canales internos de información sin estar obligadas a ello —supuesto de hecho del artículo 30.2 de la ley—, debemos circunscribirnos a entidades del sector privado que no entren en el ámbito de aplicación establecido por el artículo 10.1 de la ley, a las que solo podrá aplicarse el supuesto de legitimación determinado por el artículo 6.1.e) del RGPD.

9. No se termina de entender por qué se alude aquí a una legitimación que se circunscribe al tratamiento de datos por las autoridades públicas, cuando justamente el supuesto de hecho al que alude la revelación pública es el miedo a posibles represalias por tramitarlo por los canales internos o externos de denuncias o, entre otras, "la connivencia de una autoridad con el autor de la infracción o que esta esté implicada en la infracción". Recordemos que el ámbito de aplicación de la LO 7/2021 se ciñe a "la protección de las personas físicas en lo que respecta al tratamiento de los datos de carácter personal por parte de las autoridades competentes, con fines de prevención, detección, investigación y enjuiciamiento de infracciones penales o de ejecución de sanciones penales, incluidas la protección y prevención frente a las amenazas contra la seguridad pública" (artículo 1).

10. La única razón se podría encontrar en que en la gestación de la LOPDGDD —como recuerda la AEPD en su Informe sobre el anteproyecto de Ley 2/2023— el Consejo de Estado "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", pero, como igualmente recuerda el Gabinete Jurídico de la AEPD, tras la entrada en vigor de la Directiva 2019/1937 esa base de legitimación es otra, al quedar esta cuestión ya amparada y justificada, como acabamos de señalar, tanto en el derecho de la Unión Europea como en la normativa estatal, mediante la cláusula 6.1.c) del RGPD.

Sí tendría más sentido, sin embargo, esta doble base de legitimación del artículo 6.1.e) del RGPD y del artículo 11 de la LO 7/2021, los tratamientos de datos personales en los canales externos a los que, sin embargo, la ley legitima por la vía de este artículo 11 de la LO 7/2021, pero basándolo en el artículo 6.1.c) del RGPD y no en el apartado e) ya mencionado.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 38
ISBN: 978-84-125912-4-8

En todo caso, la cuestión es relevante y no solo meramente teórica, porque, como recuerda la AEPD a través de su Informe 0020/2022, "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 [...] se reconoce respecto de los tratamientos basados en la letra e), pero no respecto de los amparados por la letra c)".

Probablemente esta es la razón por la que el artículo 31 de la ley, en referencia al ejercicio de derechos, ha determinado en su apartado 4 que, "en el 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".

Esto es, se habilita una causa de legitimación basada en el interés público —cuando perfectamente se podía basar en la norma legal— para después reducir a cenizas el derecho de oposición que dicha base otorga a los afectados. Quizás no hacían falta tantas alforjas para tan poco viaje.

A mayor abundamiento, creo que es necesario señalar la cara menos amable de esta fijación de la licitud en la propia Ley 2/2023, por cuanto este sistema de protección que, como indica Fernández Ramos (2023), "no es apto para comunicar cualquier incumplimiento legal, sino que está constreñido a un ámbito material determinado por la ley en su artículo 2", ha excluido de su aplicación la protección en distintos supuestos, en principio regulados por otras normas, por lo que genera una suerte de carga en los sujetos obligados de verificar que las informaciones —denuncias— comunicadas a través del Sistema interno que se establezca estén en ese ámbito de aplicación normativo, de suerte que, si no lo están, corren el riesgo de estar tratando datos personales sin una base legitimadora adecuada, cuestión esta sobre la que volveremos más adelante.

Por último, en relación con la licitud de los tratamientos, es necesario hacer referencia al último apartado del artículo 30.5 de la ley, que establece que "el tratamiento de las categorías especiales de datos personales por razones de un interés público esencial se podrá realizar conforme a lo previsto en el artículo 9.2.g) del Reglamento (UE) 2016/679". El legislador ha seguido aquí las directrices del Informe del Gabinete Jurídico de la AEPD 0020/2022, sobre el anteproyecto de ley, en el que se instaba a la minimización del posible tratamiento de categorías especiales de datos, por entender que no resultaba necesario para la gestión de las comunicaciones y tramitación de los procedimientos, salvo en este supuesto específico de existencia de un

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 38
ISBN: 978-84-125912-4-8

interés público esencial, para lo que se aludía a la necesaria activación de garantías adicionales[11].

Pues bien, la propia norma solo alude a la posibilidad de tratamiento de categorías especiales de datos en relación con los sistemas internos de información para establecer 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" (artículo 32.2 de la ley).

No queda claro, entonces, si esta limitación supone que solo podrán tratarse datos personales de categorías especiales en el ámbito de los canales externos de información, o si a este precepto se debe excepcionar lo establecido por el artículo 30.5 de la ley. En todo caso, de lo que no hay duda es de que ese tratamiento de datos deberá circunscribirse a la aplicación más estricta de los principios de finalidad, necesidad y minimización, como veremos a continuación.

2.2. El cumplimiento del principio de responsabilidad proactiva

Aunque, como hemos visto, el principio de licitud preocupa sobremanera al legislador, la ley también incide en la necesidad de garantizar el resto de principios que los tratamientos han de respetar según establece el artículo 5 del RGPD, esto es, los principios de finalidad, necesidad, minimización, exactitud, confidencialidad, transparencia y responsabilidad proactiva, contemplados todos ellos de manera más o menos escueta a lo largo de la ley y, en particular, en su título VI.

De nuevo, algunas voces doctrinales han criticado una redacción meramente formal de los principios, pero quizás podría argumentarse, a este respecto, que el giro que el RGPD ha dado respecto de las obligaciones de cumplimiento de la normativa de protección de datos, más centradas en establecer la responsabilidad proactiva en los tratamientos de datos por los responsables, permite al legislador dejar más margen a los mismos para el establecimiento de las concretas medidas que garanticen dicha protección.

11. Decía específicamente el Informe 0020/2022, en alusión directa a lo regulado por el artículo 9.2.g) del RGPD: "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".

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 38
ISBN: 978-84-125912-4-8

Sin embargo, la naturaleza altamente sensible del tratamiento por los riesgos que implica y la finalidad de la norma —proteger, en todo caso, al alertador respecto de las posibles represalias que pudiera sufrir por la revelación de infracciones— requiere, desde la perspectiva del derecho a la protección de datos como un derecho instrumental y garantizador de los derechos y libertades de las personas, de unas medidas que concilien todos los elementos en juego: no solo, claro está, la protección al informador, sino también la garantía de los derechos de otras personas afectadas —posibles "señalados" por la denuncia, testigos—, la persecución de los ilícitos informados, etc.

Quizás en este sentido el amplio margen que parece dejarse en cuanto al diseño del sistema y el cumplimiento de los principios que rigen los tratamientos podría considerarse una carga excesiva que pese sobre los responsables de los sistemas de información, no solo por la obligación de implementar los sistemas de información que establece la Ley 2/2023, sino también por tener que hacerlo, en virtud del principio de responsabilidad proactiva[12], adoptando sin demasiadas directrices las medidas organizativas y técnicas necesarias para su funcionamiento, que garanticen la protección de los datos, y que a su vez permitan demostrar que dichas medidas son conformes con el RGPD.

En este sentido, el artículo 5 de la ley establece que el Sistema interno de información debe diseñarse y gestionarse de forma segura, de manera que se garantice la confidencialidad del informante y de cualquier otra persona mencionada en la comunicación, lo que se traduce, desde la perspectiva que nos ocupa, en la necesidad de cumplir con las obligaciones de la protección de datos desde el diseño y por defecto, conforme a los artículos 25 del RGPD y 32 del RGPD, es decir, con medidas jurídicas y de seguridad adecuadas que minimicen los riesgos de brechas de seguridad, por la implicación que las mismas pueden tener.

Será, por tanto, necesario llevar a cabo un adecuado análisis de riesgos periódico, previo a su implantación y durante su existencia, que tenga en cuenta tanto los mecanismos de seguridad de la plataforma —que no solo debe garantizar la posibilidad de comunicación por vía electrónica, sino

12. En los términos establecidos por el artículo 24 del RGPD, que dispone:
"Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario".

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 38
ISBN: 978-84-125912-4-8

también, como veremos, por vía verbal, mediante grabación y/o transcripción segura, así como por escrito, en papel— como los del procedimiento en sí que se regule para su gestión, permitiendo también la limitación estricta de las personas que estarán habilitadas para su llevanza, de manera que se garantice el acceso únicamente a quienes establezca la ley como posibles conocedores, en cada caso, de las denuncias, bajo un régimen de estricta confidencialidad[13].

Debemos entender, por tanto, que la naturaleza de alto riesgo de estos tratamientos obliga a los responsables de los mismos no solo al cumplimiento estricto normativo que se recoge de implantación de los canales y de gestión de las denuncias, sino a hacerlo con esa perspectiva del tratamiento de los datos desde el diseño y por defecto, y teniendo en cuenta su condición de responsables.

3. Protección de datos desde el diseño y por defecto en la implementación de los sistemas internos de información y en los procedimientos de gestión de los mismos

3.1. La determinación de los responsables y encargados de tratamiento en el marco de los sistemas internos de información y la aplicación del principio de confidencialidad en la limitación de las personas con acceso al Sistema

Uno de los aspectos básicos a determinar para la protección de los datos en los canales de denuncia es la determinación de quién ostenta la condición de responsable en estos casos. Recordemos al efecto que la Ley 2/2023 determina en su artículo 5.1 lo siguiente:

13. No está de más recordar, en este momento, que la normativa de protección de datos no solo obliga a llevar a cabo un previo análisis de riesgos aplicando el principio de la protección de datos desde el diseño y por defecto, sino que, además, obliga a llevar a cabo una específica evaluación de impacto relativa a la protección de datos (en adelante, EIPD), "cuando 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". Pues bien, la AEPD, en su informe jurídico 0020/2023, consideró de "alto riesgo" los tratamientos previstos por la ley, pero dando a entender que debía ser el propio legislador —o más bien el Gobierno y la Administración General del Estado en su propuesta de proyecto de ley— quien realizara esta EIPD a efectos de ver las garantías a las que se debiera dar traslado en el texto legal. No solo en el caso que nos ocupa, sino que la AEPD aprovechó para subrayar la necesidad de que estos análisis de riesgos y EIPD se establecieran como obligaciones legales para cualquier proyecto de ley que implique el tratamiento de datos personales.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 38
ISBN: 978-84-125912-4-8

> "El órgano de administración u órgano de gobierno de cada entidad u organismo obligado por esta ley será el responsable de la implantación del Sistema interno de información, previa consulta con la representación legal de las personas trabajadoras, y tendrá la condición de responsable del tratamiento de los datos personales de conformidad con lo dispuesto en la normativa sobre protección de datos personales".

Si bien la primera parte está clara, en cuanto a que la obligación de creación y puesta en funcionamiento —por tanto, de definición del sistema de gestión y procedimiento aplicable— corresponde al órgano de gobierno o de administración de la entidad, el hecho de que el precepto indique que este órgano "tendrá la condición de responsable de tratamiento" ha generado dudas que la AEPD ha intentado aclarar en su Informe 0054/2023 ante una consulta que, a mi juicio, con toda la razón planteaba que debe ser la entidad obligada a disponer del Sistema interno de información la responsable de los tratamientos de datos si atendemos a la definición de responsable del tratamiento del artículo 4.7 del RGPD[14].

La AEPD, tras afirmar que efectivamente la redacción del precepto viene de lo informado por ella, matiza en este informe lo siguiente:

> "La finalidad perseguida con nuestro Informe 20/2022 era contribuir a la correcta identificación de los responsables del tratamiento y de los posibles encargados, pero sin que fuera la intención de atribuir al Consejo de Administración de una sociedad mercantil una responsabilidad respecto del tratamiento de los datos personales en el Sistema interno de información diferenciada respecto de la que corresponde a la propia sociedad con relación a los restantes tratamientos de datos personales conforme al artículo 4.7 del RGPD, ni alterar el régimen de responsabilidad previsto en la normativa sobre protección de datos personales. […] Por todo ello, la correcta interpretación del artículo 5 de la Ley 2/2023, de 20 de febrero, desde la perspectiva de la protección de datos personales, requiere identificar como responsable del tratamiento a la entidad u organismo obligado por la ley a disponer de un Sistema interno

14. Resulta necesario indicar que bien está que la AEPD deshaga el entuerto causado, por cuanto ella misma fue la que sugirió que se incluyera la referencia al responsable del tratamiento en este artículo, en el citado Informe 0020/2022, en el que literalmente —y en destacado— señaló:

> "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".

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 38
ISBN: 978-84-125912-4-8

de información, sin perjuicio de que las decisiones necesarias para su correcta implantación deban adoptarse por el correspondiente órgano de administración u órgano de gobierno".

Aclarada en apariencia la cuestión[15], en el sentido de que parece que, pese a lo que literalmente diga la norma, serán las entidades las responsables de los tratamientos que se lleven a cabo, aunque sea el consejo de gobierno o de administración sobre quien pese la obligación de implementar el Sistema de información con las garantías necesarias, debe recordarse que la gestión del mismo no recae sobre este órgano, sino sobre la persona o personas concretas que se nombren como "Responsable del Sistema interno de información" en aplicación del artículo 8 de la ley, debiendo designarse facultades de gestión en una persona concreta si se opta por que el Responsable del Sistema sea un órgano colegiado.

Es importante señalar esto porque la ley permite la externalización del Sistema interno de gestión en su artículo 6, adquiriendo en este caso la condición de encargado de tratamiento, lo que no solo se deberá plasmar en el acto o contrato correspondiente —como recuerda el artículo 6.4 de la ley—, sino que recordemos que obligará a que, en su responsabilidad proactiva, la entidad responsable elija un encargado de tratamiento con todas las garantías adecuadas según establece el RGPD, lo que va más allá de la alusión por la ley en su artículo 6.2 a que "la gestión del Sistema por un tercero externo exigirá en todo caso que este ofrezca garantías adecuadas de respeto de la independencia, la confidencialidad, la protección de datos y el secreto de las comunicaciones".

El alcance de esa externalización parece quedar acotado en el artículo 6.1 de la ley a un mero apoyo técnico para la recepción de las informaciones, al establecerse que "la gestión del Sistema interno de información se podrá

15. Decimos "en apariencia" porque, dado el tenor literal del precepto, si aplicamos estrictamente el artículo 4.7 del RGPD no queda tan clara esta cuestión, porque se define al "responsable del tratamiento" o "responsable" como "la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el derecho de la Unión o de los Estados miembros".

Si bien supera el ámbito de este trabajo, no está de más plantearse que la interpretación de la AEPD, aunque muy voluntarista, no sea suficiente para entender a las entidades como responsables, si tenemos en cuenta que los fines —la protección de los informantes y el interés público en la persecución de infracciones del derecho de la Unión— y medios del tratamiento —los canales de denuncia— vienen directamente establecidos por el legislador, que ha designado, en apariencia, al órgano de gobierno o de administración como responsable. Sería conveniente plantear la necesidad de reformar este artículo para que, con mayor seguridad jurídica, establezca la condición de responsable de la entidad, que es lo lógico en estos casos.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 38
ISBN: 978-84-125912-4-8

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".

Este artículo, que se complementa por el artículo 15 de la ley en el mismo sentido para el sector público, parece dar a entender que esta figura será en todo caso un proveedor que proporcione herramientas de *software* o servicios en la nube para la recepción de la información, reforzándose esta idea en el artículo 6.3, que concreta que "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 esta ley ni una atribución de la responsabilidad sobre el mismo en persona distinta del Responsable del Sistema previsto en el artículo 8".

Por último, es necesario señalar que el artículo 6.2 prevé la posibilidad de existencia de corresponsables —lo que exigirá la suscripción del acuerdo correspondiente, conforme al artículo 26 del RGPD—, figura en todo caso aplicable a situaciones como las recogidas en los artículos 12 y 14, que permite a pequeñas empresas o Administraciones, respectivamente, compartir el Sistema interno de información, pero cumpliendo con las garantías de confidencialidad de la norma, es decir, que si bien comparten los fines y medios del tratamiento, cada entidad deberá tener acceso exclusivo a las informaciones que le afecten.

Respecto de las personas físicas encargadas de la gestión del Sistema, debemos señalar cómo la ley limita de manera categórica las personas que pueden tener acceso a la información del Sistema, en aplicación de los principios de necesidad y de confidencialidad[16], a fin de reforzar los mecanismos de protección de los informantes, de tal manera que incluso cuando se nombra como responsable de un Sistema interno a un órgano colegiado, "este deberá delegar en uno de sus miembros las facultades de gestión del Sistema interno de información y de tramitación de expedientes de investigación" (artículo 8.2), reforzando el carácter de su gestión independiente y autónoma (artículo 8.4), evitando los conflictos de interés, en su caso (artículo 8.5), y pudiendo designarse al oficial de *compliance* de existir ya en la organización (artículo 8.6 de la ley).

16. Así lo había señalado ya el Supervisor Europeo de Protección de Datos en sus *Guidelines on procession personal information within a whistleblowing procedure*, publicadas en diciembre de 2019, indicando que "*internal access to the information processed as part of the investigation of the allegations must be granted strictly on a need to know basis, in other words, subject to necessity. Those in charge of the management of reports could, for example, be subject to a reinforced obligation of secrecy*".

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 38
ISBN: 978-84-125912-4-8

La ley limita categóricamente las personas que pueden tener acceso a los datos personales que se traten junto con la información, estableciendo en su artículo 32.1 lo siguiente:

> "1. El acceso a los datos personales contenidos en el Sistema interno 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 o el órgano competente debidamente designado, solo 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".

Esto implica además una compartimentación estricta de las personas con acceso a la información en cada situación, de manera que solo podrán tenerlo, en aplicación del principio de minimización, cuando la naturaleza de la información requiera de su intervención. Y lo mismo cabe decir respecto de las cesiones de datos, que el mismo artículo 32.2 considera lícitas "cuando resulte necesario para la adopción de medidas correctoras en la entidad o la tramitación de los procedimientos sancionadores o penales que, en su caso, procedan".

Se refuerza, además, esta idea de confidencialidad en el artículo 9.2.g) de la ley, al establecer, aunque con una sistemática un tanto discutible, que el procedimiento de gestión de las informaciones responderá, entre otros, al siguiente principio:

> "g) Garantía de la confidencialidad cuando la comunicación sea remitida por canales de denuncia que no sean los establecidos o a miembros del personal no responsable de su tratamiento, al que se habrá formado en esta materia y advertido de la tipificación como infracción muy grave de su quebranto y, asimismo, el establecimiento de la obligación del receptor de la comunicación de remitirla inmediatamente al Responsable del Sistema".

3.2. Finalidad, integridad y transparencia

Otra de las cuestiones sobre las que es interesante reflexionar a la hora de la implementación del Sistema interno de información es sobre la finalidad de dicho canal, que no puede ser, en principio, un genérico buzón para todo tipo de quejas o incumplimientos, al limitarse, como ya hemos visto, el ám-

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 38
ISBN: 978-84-125912-4-8

bito material de protección en el artículo 2 de la ley. De hecho, la propia ley establece en su artículo 7.4 la posibilidad de que a través de esos canales se puedan recibir informaciones y comunicaciones fuera del ámbito que establece el mencionado artículo 2; tanto esas comunicaciones como quienes las remitan no gozarán de la protección de la Ley 2/2023.

En todo caso, el artículo 5.2 enumera las características que deben reunir estos sistemas internos de información[17], que sin duda plantean elementos de transcendencia en relación con la protección de datos desde el diseño y por defecto, mediante sistemas seguros y políticas apropiadas para garantizar un auténtico hermetismo del sistema.

Las medidas de seguridad, además, deberán preverse en función de los requisitos y posibilidades de comunicación que prevé el artículo 7.2 de la ley, con posibilidad de grabación y/o transcripción de la información, debiendo implementarse tanto controles de accesos para todos estos supuestos como medidas adecuadas para su conservación y/o supresión en su caso, y por supuesto, todo ello previa información a los interesados de que tratamientos que se vayan a llevar a cabo pueden implicar la grabación, transcripción o documentación de los intercambios de información que se produzcan, y deben permitir el ejercicio de los derechos de acceso y rectificación en todo caso[18].

17. Señala este artículo 5.2 de la Ley 2/2023:

"El Sistema interno de información, en cualquiera de sus fórmulas de gestión, deberá:

a) Permitir a todas las personas referidas en el artículo 3 comunicar información sobre las infracciones previstas en el artículo 2.
b) Estar 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.
c) Permitir la presentación de comunicaciones por escrito o verbalmente, o de ambos modos.
d) Integrar los distintos canales internos de información 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 la propia entidad u organismo.
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 14.
g) Contar con un Responsable del Sistema en los términos previstos en el artículo 8.
h) Contar con una política o estrategia que enuncie los principios generales en materia de Sistemas interno 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 informaciones 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".

18. Aunque la ley hable de garantizar el ejercicio por los interesados de "los derechos a que se refieren los artículos 15 a 22" del RGPD (artículo 31.3 de la ley), es obvio, como hemos visto,

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 38
ISBN: 978-84-125912-4-8

Huelga decir que la implementación de un canal de estas características, con garantías suficientes para la preservación de la información, la supresión cuando sea necesario y, sobre todo, la protección de la identidad de los informantes, requiere de esfuerzos técnicos importantes que no todas las entidades podrán asumir, lo que está generando ya una importante oferta de encargados de tratamiento para proveer de soluciones informáticas para implantar mecanismos que cumplan con las obligaciones de la ley. No obstante, como hemos visto, seguía pesando sobre los responsables la obligación de velar por el adecuado cumplimiento de los principios de protección de datos, mediante sistemas y controles que garanticen el posible anonimato y la confidencialidad de la identidad del informante, así como la exactitud de los datos —en la grabación o su transcripción—, la posible minimización de los mismos —con la consiguiente supresión de los que no sean estrictamente necesarios en relación con la información—, y la inclusión de información suficiente a los interesados sobre el tratamiento de datos que se va a hacer, puesto que el rol de encargado de tratamiento no incluye la gestión de la información, sino solo su recepción.

Como garantía adicional de transparencia, además de informar sobre la protección que dispensa el canal y los derechos de los interesados en el tratamiento de sus datos, conforme al artículo 31 de la ley, sería conveniente dar de alta el Sistema de información interno como tratamiento específico de datos en el Registro de Actividades de Tratamiento (RAT), especialmente por lo que se refiere a las entidades del sector público, pues, como indica Ricard Martínez (2023), "se trata de un tratamiento cuya finalidad y características esenciales vienen definidas por la ley para la persecución de fines de interés público y la garantía de los derechos de las personas denunciantes. La capa adicional de transparencia que se impone al RAT de las administraciones permite incrementar la proactividad en la garantía de este principio".

3.3. Tratamiento de los datos personales en el procedimiento de gestión de la información

El Supervisor Europeo de Protección de Datos ha señalado, en sus "Orientaciones sobre los mecanismos de denuncia de infracciones"[19], la necesidad de definir el alcance del procedimiento de denuncia de la manera lo más limitada posible, en cada caso, para evitar el abuso del mecanismo, indicando

que no todos ellos pueden ser de aplicación en este supuesto, ni su ejercicio por todos los interesados.

19. Supervisor Europeo de Protección de Datos (EDPS) (2019: 6).

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 38
ISBN: 978-84-125912-4-8

claramente que los canales de información no deben ser usados para otras finalidades que tienen sus propias vías de ejercicio. Se trata de minimizar los datos personales objeto de tratamiento a los estrictamente necesarios.

Esto entronca con una de las obligaciones que hemos visto pesa sobre los responsables en su implantación del Sistema interno de información, que no solo deben "contar con un procedimiento de gestión de las informaciones recibidas", sino que el mismo debe "contar con una política o estrategia que enuncie los principios generales en materia de Sistema interno de información y defensa del informante y que sea debidamente publicitada en el seno de la entidad u organismo". De nuevo, la necesidad de un diseño previo de los procedimientos entronca directamente con la idea de la protección de datos desde el diseño en el ámbito de la responsabilidad proactiva de los sujetos obligados, que deberán establecer no solo las vías o los canales de recepción de la información, sino también, específicamente, procedimientos claros para gestión de las denuncias, sobre los que también deberán ser transparentes y dar información clara a los interesados.

Cada entidad parece que puede diseñar este procedimiento como le parezca oportuno[20], teniendo en cuenta, además, que será el Responsable del Sistema —o la persona en que se delegue— quien deba hacer esta tramitación, por cuanto, como hemos visto, los encargados del tratamiento solo lo son para la recepción de las informaciones.

En cualquier caso, la ley establece ciertas obligaciones sobre el procedimiento de gestión de informaciones, al que dedica su artículo 9, e indica cuestiones concretas en relación con el tratamiento de datos que se haga en dicho procedimiento, además de contener una remisión específica a lo previsto en el título VI (artículo 9.2.i) para el tratamiento de los datos personales. Nos vamos a detener, aunque sea brevemente, en algunas de estas previsiones.

En primer lugar, el informante que activa el procedimiento mediante su comunicación de una información —que puede optar por el anonimato— tiene una protección reforzada, de tal manera que la ley establece, en su artículo 33.3, que su identidad solo puede ser comunicada a la Autoridad judicial, al Ministerio Fiscal o a la autoridad administrativa correspondiente, siendo necesario trasladar al informante notificación de dicha revelación de su identidad, salvo que pudieran verse comprometidos la investigación o el procedimiento judicial, debiendo motivarse dicha revelación.

20. Y en aplicación, como hemos visto, del principio de responsabilidad proactiva.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 38
ISBN: 978-84-125912-4-8

Obviamente, el informante debe tener conocimiento, antes de usar el Sistema de información, de qué cauces dispone para hacer su comunicación[21], así como de cómo van a ser tratados sus datos personales y de los derechos que le asisten, como ya hemos visto.

Al respecto, recordemos que el artículo 7.2 de la ley establece que "el canal interno deberá permitir realizar comunicaciones por escrito o verbalmente, o de las dos formas. La información se podrá realizar bien por escrito, a través de correo postal o a través de cualquier medio electrónico habilitado al efecto, o verbalmente, por vía telefónica o a través de sistema de mensajería de voz. A solicitud del informante, también podrá presentarse mediante una reunión presencial dentro del plazo máximo de siete días".

En el uso de estos canales, el denunciante debe ser informado de que su comunicación, de ser verbal, será grabada, e igualmente de que dispone también de canales externos de información, por si decide optar por estos.

Junto a esta información, al informante se le deberá dar toda la información relativa al tratamiento, conforme a lo establecido en los artículos 13 y siguientes del RGPD, respecto del responsable, la finalidad, los destinatarios, en su caso, los plazos de conservación, los derechos que le asisten, y las medidas de seguridad implementadas[22].

El artículo 31 de la ley, dedicado específicamente a la "información sobre protección de datos personales y ejercicio de los derechos", poco viene a complementar, en este sentido, lo establecido por el artículo 13 del RGPD, al que se remite, más allá de indicar que a los informantes se les informará, "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"; y el posible ejercicio de los derechos regulados por los artículos 15 a 22 del RGPD.

En este sentido, la sistemática de la ley es algo confusa, pues, como hemos visto, la misma prevé la remisión de la información —con sus datos personales— a las autoridades pertinentes en el marco de una investigación (artículo 33 de la ley), de lo que se deberá dar oportuna información al infor-

21. Véase, al respecto, lo previsto en el artículo 25 de la ley, relativo a la información sobre los canales interno y externo de información.

22. Esta información, como acabamos de ver, debe constar también en el registro de actividades de tratamiento, conforme al artículo 31 RGPD, por lo que se podrá remitir al mismo como información de segunda capa, siempre que esté publicada —como debe ser el caso para las entidades del sector público, conforme a lo establecido por el artículo 7 bis de la Ley 19/2013, de transparencia, acceso a la información pública y buen gobierno—.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 38
ISBN: 978-84-125912-4-8

mante; y que, al estar legitimado el tratamiento en la base de licitud del artículo 6.1.c) del RGPD, su derecho de oposición está, cuando menos, limitado.

En cuanto a la protección que recibe el informante, también debe tenerse en cuenta que la misma se produce en el ámbito de la finalidad de la ley y no más allá, por cuanto el artículo 7.4 de la ley establece que "los canales internos de información podrán estar habilitados por la entidad que los gestione para la recepción de cualesquiera otras comunicaciones o informaciones fuera del ámbito establecido en el artículo 2, si bien dichas comunicaciones y sus remitentes quedarán fuera del ámbito de protección dispensado por la misma".

Es decir, que habrá de darse información clara al informante de que su identidad puede no quedar protegida si lo que denuncia o comunica queda fuera de las finalidades de la ley, siendo, como ya hemos visto, una carga adicional del gestor del sistema, que deberá determinar qué informaciones entran dentro del ámbito de protección de la ley, y cuáles no.

No es la única carga que pesa sobre el Responsable del Sistema a la hora de gestionar las informaciones recibidas: el artículo 32 de la ley, dedicado al tratamiento de datos personales en el Sistema interno de información, al que ya nos hemos referido, establece una serie de obligaciones, *a priori* acordes con los principios relativos al tratamiento establecidos por el artículo 5 del RGPD, pero que pueden ser de difícil cumplimiento por las entidades.

En primer lugar, en aplicación del principio de minimización, el artículo 32.2 dispone lo siguiente:

> "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. 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".

Esto es, el Responsable del Sistema deberá decidir si los datos personales —del informante y de otras personas a las que se pueda aludir en la denuncia— son o no necesarios, y si entran o no en el ámbito de aplicación de la ley, lo que no es, en todo caso, fácil de determinar.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 38
ISBN: 978-84-125912-4-8

Además, también deberá proceder a la supresión —"inmediata", dice la ley— de los datos relativos a categorías especiales, aunque aquí habrá que entender que puede ser aplicable la excepción establecida en el artículo 9.2.g) del RGPD, en aplicación del artículo 30.5 de la ley, a lo que ya nos hemos referido, siendo esta también una carga adicional para el Responsable del Sistema.

Pero es que, además, este artículo 32 va más allá, porque su apartado 3, después de aludir al principio de mínima conservación temporal de los datos —sobre lo que volveremos ahora—, establece lo siguiente:

> "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, salvo que dicha falta de veracidad pueda constituir un ilícito penal, en cuyo caso se guardará la información por el tiempo necesario durante el que se tramite el procedimiento judicial".

Cómo se deba hacer ese "juicio de veracidad" de la información, es difícil de determinar. No queda claro si el Responsable del Sistema debe aventurar una primera valoración, o si la misma debe quedar acreditada en vía judicial, si la supresión por tanto es previa a la investigación o si es resultado de la misma, cuestión que tendría más sentido, puesto que no creo que se pueda cargar al Responsable del Sistema con la responsabilidad de determinar si la falta de veracidad puede o no constituir un ilícito penal.

Todo ello teniendo en cuenta, además, que en el tratamiento de los datos personales en la gestión de las informaciones no solo se trata de proteger la identidad del informante, sino cualesquiera otros datos personales que comunique, sean del informante o de terceros, haciendo más difícil si cabe la aplicación estricta del principio de minimización.

Volviendo, por último, sobre la cuestión de los plazos de conservación de los datos personales, fuera de estos ámbitos de supresión inmediata —inmediatez que, como vemos, puede no referirse al momento de recepción de la información, sino de verificación de la necesidad de los datos o de su falta de veracidad— la ley contiene varias referencias a los plazos de conservación de los datos personales.

De un lado, la ley estipula, en su artículo 32.3, lo que Fernández Salmerón (2023: 209) ha denominado "principio de prudencia cronológica", al establecerse que "los datos que sean objeto de tratamiento podrán conservarse en el sistema de informaciones únicamente durante el tiempo impres-

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 38
ISBN: 978-84-125912-4-8

cindible para decidir sobre la procedencia de iniciar una investigación sobre los hechos informados".

De otro, el artículo 32.4 establece que el plazo de conservación de la comunicación, salvo que se anonimice, será de tres meses cuando no se hubieran iniciado actuaciones de investigación, no siendo de aplicación el bloqueo de los datos previo a su supresión, sino la supresión directa,

Obviamente, la iniciación de las actuaciones de investigación no debe ser una cuestión discrecional para la entidad, o para el Responsable del Sistema de información interno —y así se establece en el artículo 7 de la ley, que da justamente el mismo plazo de tres meses para "dar respuesta a las actuaciones de investigación", salvo que sea necesaria una ampliación de plazo—, pero parece establecerse aquí una suerte de caducidad del plazo del procedimiento de investigación.

En todo caso, debe entenderse que esta supresión no podrá ser usada a modo de fraude por parte de las entidades para eludir su responsabilidad en la investigación de los ilícitos[23], quedando no solo registro obligatorio de la comunicación de informaciones mediante el libro-registro previsto por el artículo 26 de la ley, sino habilitando al informante a quedar protegido en el caso de que decida hacer una revelación pública de la información cuando las informaciones no sean investigadas (artículo 28.1.a de la ley), y estando además tipificado como infracción muy grave "cualquier intento o acción efectiva de obstaculizar la presentación de comunicaciones o de impedir, frustrar o ralentizar su seguimiento" (artículo 63.1.a de la ley).

A modo de cierre del Sistema, el artículo 26 recuerda la necesidad de cumplimiento de este principio de limitación del plazo de conservación que establece el artículo 5.1.e) del RGPD, determinando que solo se conservarán los datos personales relativos a informaciones e investigaciones "durante el período que sea necesario y proporcionado a efectos de cumplir con esta ley", estableciéndose de forma tajante que "en ningún caso podrán conservarse los datos por un período superior a diez años" (artículo 26.2 de la ley).

Por último, para finalizar este estudio, resulta de interés referirse a la figura del delegado de protección de datos (DPD), como figura de asesoramiento y supervisión en materia de protección de datos, que la ley incluye

23. Evidentemente las obligaciones de tramitación no son las mismas para las entidades públicas, para las que este procedimiento tendrá —entiendo— la condición de procedimiento administrativo, y deberán aplicarse las previsiones de la Ley 39/2015, de procedimiento administrativo común de las Administraciones públicas.

Fundación Democracia y Gobierno Local
Serie: Claves del Gobierno Local, 38
ISBN: 978-84-125912-4-8

como obligatoria para la Autoridad Independiente de Protección del Informante y las autoridades independientes que en su caso se constituyan, según el artículo 34 de la ley. Sin embargo, son muchas las entidades públicas y privadas que, estando obligadas a implantar los sistemas internos de información, tienen la obligación de contar con un DPD, en aplicación de lo previsto por el RGPD y la LOPDGDD, y así se refleja en la posibilidad de que tengan acceso —como no podría ser de otra manera— a los datos personales contenidos en el Sistema interno de información, en el artículo 32.1.e) de la ley.

El o la DPD no tendrá solo un rol en la gestión de las informaciones para garantizar la protección de los datos de los interesados, sino que también deberá participar, mediante su asesoramiento y supervisión, en la protección de datos desde el diseño y por defecto de estos canales, por cuanto ya sabemos que la protección de datos requiere de una gestión de riesgos dinámica, en la que de manera periódica se revisen las medidas jurídicas y técnicas para garantizar la protección de datos en los sistemas internos de información, así como en los sistemas externos de información, cuando estos se pongan en marcha.

Contar con el apoyo del/de la DPD será de gran utilidad para la aplicación de una norma que, como hemos visto, deja un gran margen de actuación a las entidades obligadas, que deberán diseñar los mecanismos jurídicos y técnicos más adecuados para la protección de los datos personales que deban tratarse, en su caso, en los procedimientos de denuncia que se inicien en aplicación de la Ley 2/2023.

4. Bibliografía

Fernández Ramos, S. (2023). Ley 2/2023, de 20 de febrero, de protección al informante: ámbito material de aplicación. *Revista General de Derecho Admninistrativo*, 63.

Fernández Salmerón, M. (2023). La protección de datos personales. En J. M.ª Pérez Monguió y S. Fernández Ramos (coords.). *El nuevo sistema de protección del informante*. Bosch.

Martínez Martínez, R. (2023). El tratamiento de datos personales en el marco de la Ley 2/2023, de protección del denunciante. Requisitos y recomendaciones para el sector público. *La Ley privacidad*, 15.

Piñar Mañas, J. L. (2020). La transposición de la Directiva relativa a la protección de las personas que informen sobre infracciones del derecho de la Unión. *Anuario del Buen Gobierno y de la Calidad de la Regulación 2019*.

ISBN: 978-84-125912-4-8

Sempere Samaniego, F. J. (2021). La licitud del tratamiento. (Comentario al artículo 6 RGPD y 8 LOPDGDD y Disposición adicional duodécima LOPDGDD). En A. Troncoso Reigada (dir.). *Comentario al Reglamento General de Protección de Datos y a la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales*. Thomson Reuters-Civitas.

Supervisor Europeo de Protección de Datos. (EDPS). (2019). *Guidelines on procession personal information within a whistleblowing procedure*. Disponible en: https://edps.europa.eu/data-protection/our-work/publications/guidelines/guidelines-processing-personal-information-within_en.