LOS SISTEMAS INTERNOS DE INFORMACIÓN EN LA LEY 2/2023 DE PROTECCIÓN DE PERSONAS INFORMANTES: UN ANÁLISIS JURÍDICO ANTE SU INMEDIATA EXIGIBILIDAD*

THE WHISTLEBLOWER PROTECTION LAW AND INTERNAL INFORMATION SYSTEMS: A REVIEW FOR ITS IMMEDIATE IMPLEMENTATION

Javier Sierra-Rodríguez
Profesor del Departamento de Derecho Constitucional
UNED
javier.sierra@der.uned.es

https://doi.org/10.47623/ivap-rvgp.24.2023.03

Recibido: 20/03/2023 Aceptado: 16/05/2023

Nota: Conforme a las políticas de la Revista Vasca de Gestión de Personas y Organizaciones Públicas se ha redactado el artículo teniendo en cuenta la utilización de un lenguaje no sexista. No obstante, en algunos pasajes no se ha podido llevar a cabo, debido a que la utilización de términos o construcciones alternativas no permitirían mantener intacto el sentido que se quiere expresar en el texto, además de evitar que se dificulte su lectura.

Laburpena: Zuzenbideko arau-hausteei buruzko informatzaileak babesteari buruzko otsailaren 20ko 2/2023 Legea funtsezko urratsa da sektore publiko eta pribatuko irregulartasunei buruzko informazioa biltzeko sistemak abian jartzeko. Artikulu honen bidez, legearen lehen irakurketa kritikoa egin nahi da legearen eremu materialari eta aplikatu beharreko eremu pertsonalari buruz, bai eta erakundeen barruan egon behar duten barne-informazioko sistemak osatzen dituzten elementuei ematen zaien konfigurazioari buruz ere. Edukiak sektore publikoarentzako inplikazioei arreta berezia eskainiz aztertzen dira, eta, testuan zehar, gogoeta egiten da barne-informazioko sistema horiek arrakastaz ezartzeko aurre egin beharreko erronkei buruz. Testua amaitzeko, gogoeta batzuk egiten dira, barne-sistema horiek behar bezala funtziona dezaten funtsezkotzat jotzen diren elementuetan arreta jartzeko. Sistema horietan, sistemaren arduradunak rol protagonista hartzen du, informazioa tratatzeko eta haren jarraipena egiteko prozedurak zehazten dira, eta informatzailea babesteko agintaritza independenteak kanpotik egin behar duen lana zehazten da.
Gako-hitzak: Alertak, informatzaileak, informatzaileak babestea, 2/2023 Legea.

Abstract: The Spanish Law 2/2023, on the protection of whistleblowers regarding violations of law, constitutes a transcendental step for the implementation of systems for capturing information on irregularities in the public and private sectors.This article tries to carry out a first critical reading of its contents, regarding its material and subjective scope of application, and delves into the elements that make up internal information systems within organizations. The contents are analyzed with special attention to the implications for the public sector and throughout the text we reflect on the challenges that must be faced for the successful implementation of these internal systems.The text concludes with a series of reflections that focus on the elements that are considered key for these internal systems to function correctly, in which acquires a leading role the figure of the person in charge of the system, the specific procedures for handling and monitoring information, and the work that the independent whistleblower protection agency must carry out from outside.
Keywords: Law 2/2023, reporting channels, whistleblowers, whistleblowers protection.

Resumen: La Ley 2/2023, de 20 de febrero, de de protección de personas informantes sobre infracciones de Derecho constituye un paso trascendental para la puesta en marcha de los sistemas de captación de información sobre irregularidades en el sector público y privado. Este artículo trata de realizar una primera lectura crítica de la Ley respecto a su ámbito material y personal de aplicación, y sobre la configuración que se otorga a los elementos que componen los sistemas de información interna que deben existir en el seno de las organizaciones. Sus contenidos se analizan con una especial atención a las implicaciones para el sector público y, a lo largo del texto, se reflexiona sobre los retos a afrontar para la implantación exitosa de estos sistemas de información interna. El texto concluye con una serie de reflexiones que ponen el foco en los elementos que se consideran clave para que funcionen correctamente estos sistemas internos, en los que adquiere un rol protagonista la persona responsable del sistema, la concreción de los procedimientos para el tratamiento y seguimiento de la información, y la labor que debe desempeñar desde fuera la Autoridad Independiente de Protección del Informante.
Palabras clave: Alertas, Ley 2/2023, personas informantes, protección de informantes.

* Este artículo ha sido elaborado en el marco del Proyecto PID2021-128309NB-I00 «La conciliación del derecho a la protección de datos con el cumplimiento por los poderes públicos del deber de transparencia y de lucha contra la corrupción» (DATATRANSCO) financiado por el MICIN - Agencia Estatal de Investigación.

Sumario:

1. Introducción

En febrero de 2023 y con más de un año de retraso respecto a la fecha fijada para la trasposición de 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* (en adelante la Directiva)[1], quedaba aprobada 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* (en adelante la Ley).

Durante este periodo hasta su aprobación —también con anterioridad— se habían creado amplias expectativas sobre esta regulación, dado el amplio impacto que se espera en términos de prevención y detección de irregularidades. Sin embargo, no solo por eso, sino porque como afirmaba el profesor Villoria Mendieta (2021a p. 17) con relación a la Directiva: «la norma afecta a miles de organizaciones, a millones de personas insertas en tipos de organizaciones muy diversos y conlleva un cambio organizativo y cognitivo bastante profundo» [2]. Efectivamente su alcance abarca a los sectores público y privado y conlleva —o debería conllevar— un cambio cultural sobre lo que hasta ahora se identificaba con el hecho de denunciar[3].

Bajo este marco, el objetivo que nos fijamos en las siguientes páginas es hacer una lectura crítica de los contenidos de la Ley, confrontando el texto finalmente aprobado con el margen que permitía la Directiva y con las diversas posiciones que desde la doctrina se han mostrado durante el proceso prelegislativo y legislativo, a lo que se añadirán reflexiones que se suscitan sobre su implementación.

Por razones de espacio, y aunque se abordarán los fundamentos y elementos básicos de la regulación (panorama general, ámbito de aplicación material y personal), nos centraremos, particularmente, en lo que se vienen a denominar como sistemas internos de información. Todo ello, se hará con especial atención al ámbito público.

Para cumplir con este propósito, tras esta introducción se desarrollan algunas consideraciones generales sobre los fundamentos que sustentan los canales de denuncia, así como sobre el esquema global de los sistemas de información, para, a continuación, centrar el examen de contenidos en el ámbito material y personal de aplicación. Seguidamente se profundizará en los elementos que forman parte del sistema interno de información, es decir, en el conjunto que conforman las siguientes piezas: canales internos de alerta, las políticas y procedimientos de gestión de la información y la figura del responsable del sistema, culminando todo ello con unas reflexiones finales.

Antes de dar por cerrada esta introducción, se advierte que utilizaremos indistintamente los términos denunciante e informante y sus distintas variaciones, pero, principalmente, recurriremos a la expresión «alertador» porque nos parece más inteligible que la opción escogida por el legislador.

Núm. 24 zk./2023. Págs. 70-98 or.
ISSN: 2173-6405 e-ISSN: 2531-2103

2. Alertas y protección: el porqué de las cosas

De manera preliminar, conviene hacer un breve repaso a algunos de los fundamentos que nos han llevado hasta aquí. En España, las infracciones administrativas, penales y de otra naturaleza cuentan con diversos cauces reconocidos en el ordenamiento para su denuncia, pero se han mostrado insuficientes como mecanismo para desvelar eficazmente todas las conductas que quebrantan el ordenamiento jurídico (Pérez Monguió, 2020 p. 228).

En el ámbito administrativo, por ejemplo, el artículo 62 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común y de las Administraciones Públicas (LPAC), prevé la iniciación de procedimientos administrativos mediante denuncia, pero la persona denunciante deberá estar indentificada y no adquirirá la condición de interesada en el procedimiento. Bajo estas estipulaciones, ni se asegura la confidencialidad, ni quien se anima a hacer la denuncia obtiene un estatus que le permita saber qué está ocurriendo tras ella, o gozar de algún tipo de protección específica. Así las cosas, las condiciones que se establecían de manera generalizada para este tipo de denuncias no incentivan su utilización[4].

En un paso más hacia la detección y disuasión de la comisión de infracciones, se ha estado debatiendo de manera continuada en instituciones supranacionales sobre los sistemas que permitan captar información para atajarlas, prestando atención a modelos procesales distintos como el estadounidense (Fernández López, 2018 p. 263). En esta línea, algunas comunidades autónomas y municipios han hecho un *sorpasso* al Estado al avanzar hacia la regulación de los canales de denuncia (Sierra Rodríguez, 2020a p. 14)[5].

En cualquier caso, ha sido la Directiva el hito fundamental que ha forzado la adopción de una ley estatal de alcance generalizado en nuestro país. Con su aprobación se buscaba que, en los países de la UE y a través de su transposición, se generalizase un sistema para canalizar la información sobre infracciones de derecho en los ámbitos público y privado y permitir su posterior seguimiento. Todo ello mediante el diseño de un sistema de recepción de información, pero, principalmente, abordando una cuestión nuclear como es la protección de quienes pueden facilitarla.

Como se ha avanzado, estos sistemas tienen en su centro a la figura del alertador bajo una doble perspectiva. Por un lado, se pretende captar la información sobre las infracciones que quedan más alejadas de cualquier conocimiento y que se desarrollan en ámbitos reducidos —en el interior de las organizaciones—, cuyas posibilidades de ser conocidas se limitan a que sea una persona de la misma organización quien las desvele (Miranzo Díaz, 2019 p. 364). La traducción de este planteamiento por la Directiva es su orientación hacia quienes tienen conocimiento de infracciones en el marco de una relación laboral o asimilada. Por otro lado, en consonancia a este tipo de vinculación, se exige como contrapartida que se ofrezca un marco de seguridad y protección la persona denunciante, de modo que esta se vea arropada ante las posibles represalias y se anime a denunciar. Hay que recordar que, en un marco laboral, las formas de represalia pueden ser sutiles y casi invisibles[6], por lo que es necesario adoptar medidas, tanto para prevenir este tipo de reacciones, como para que cesen o se reparen las que se pudieran estar produciendo[7].

Con todo, la protección para el informante se desplegará siempre que se cumplan con unas condiciones, como utilizar los cauces establecidos para «informar» y que la información ostente las cualidades que se esperan de quien obra de buena fe para señalar las infracciones. Así, la Directiva, y ahora la Ley, construyen un sistema de canales preestablecidos para comunicar la información, cuya diferenciación se articula en función de su carácter interno —en el seno de cada organización—, o externo, como una vía ajena a la organización en la que se producen los incumplimientos y que será gestionada por una Autoridad Independiente de Protección del Denunciante o por sus equivalentes autonómicos. La utilización del canal interno se dibuja como la vía prioritaria, pero no excluye la posibilidad de que los alertadores acudan directamente a la vía externa. De hecho, tal y como se deducía del esquema planteado por la Directiva, la persona informante tiene plena libertad para acudir a una vía u otra (Bachmaier, 2019). Adicionalmente, se prevé la protección ante la difusión pública siempre que se cumplan algunas condiciones, como haber realizado la alerta a través de los canales anteriores sin que se adopten medidas o porque se prevea como perjudicial o existan riesgos inminentes; o bien, porque la alerta se haga en el marco del ejercicio de la libertad de expresión e información teniendo como destinataria a la prensa.

Estos son los rasgos básicos de esta Ley, que se desarrolla a partir de un extenso preámbulo que nos ayuda a contextualizar el sistema que se establece a lo largo de sus 68 artículos distribuidos en 9 títulos[8]. Éstos vendrán acompañados de una serie de disposiciones entre las que se recoge la modificación de siete leyes en coherencia a los contenidos de la Ley[9]. En general y antes de entrar en el análisis del ámbito material y subjetivo de aplicación, es conve-

niente indicar que estamos ante una norma compleja por lo impreciso de su articulado, que se limita en muchos casos a la mera reproducción de la Directiva utilizando otros términos, y sin que termine de armar de una manera completa la configuración de los diferentes sistemas de información y protección. Por ello, no es suficiente por sí sola para conocer el verdadero alcance de todas las obligaciones que impone, y origina que sea necesario consultar de manera constante su preámbulo y acudir a la Directiva que transpone para buscarle un sentido a muchas de sus previsiones.

3. El ámbito material de aplicación: el entrecruzamiento entre las infracciones de Derecho de la Unión y las calificadas como graves o muy graves en el ámbito administrativo y penal

Uno de los defectos que podría haber tenido la Ley deriva del acotamiento que la Directiva hacía de su ámbito de aplicación material. En lógica coherencia con las competencias comunitarias, lo proyectaba sobre las infracciones relativas a actos normativos de la Unión de una enumeración de ámbitos y materias[10], ampliada a expresiones de mayor alcance como las infracciones que tengan afectación a los intereses financieros de la Unión o al mercado interior[11]. En todo caso, se dejaba en manos de los Estados la ampliación del ámbito de protección —art. 2.2 de la Directiva—, posibilidad que aprovechó el legislador interno para extenderlo a aquellas infracciones de derecho de carácter penal y administrativo que estén calificadas como graves o muy graves, con mención expresa de aquellas de idéntica calificación que «impliquen quebranto económico para la Hacienda Pública y para la Seguridad Social» —art. 2.1 *b)*—.

La solución aportada por la Ley nacional acoge una fórmula, cuya limitación en función de la gravedad se viene a justificar, según el preámbulo de la Ley, para luchar contra las infracciones que mayor impacto tienen. Se puede intuir que, con ello, el legislador también busca economizar los esfuerzos, dado que una apertura absoluta sobre aquello que se puede denunciar y que da acceso a protecciones, es previsible que terminase provocando una saturación de los sistemas de alerta en grandes organizaciones, particularmente, de la vía alternativa que constituyen los canales externos y que acapararán las alertas del sector público y privado que no sean absorbidas en el interior de las organizaciones. Todo ello, sin perjuicio de que unas pocas autoridades independientes —la estatal y las que se prevean en cada comunidad autónoma— son las que están llamadas a asumir el protagonismo en la prestación de las medidas de apoyo a los alertadores (art. 41).

Se podría defender que este sistema basado en la gravedad de las infracciones minora —por su carácter transversal— que la persona denunciante tenga la necesidad de conocer con exactitud si el sector en el que se producen está cubierto por el sistema de protección, algo que ya fue señalado por la doctrina como un problema si la transposición se limitaba al ámbito material dispuesto por la Directiva (Bachmaier, 2019). En efecto, la opción adoptada por el legislador español es positiva en comparación al acotamiento mínimo que estaba preceptuado por la Directiva, pero a mi juicio, sigue siendo insuficiente, porque da espacio a la incertidumbre sobre qué se puede denunciar, aunque más o menos se pueda intuir qué es y qué no es grave. Es cierto que estamos ante un ámbito material más extenso porque se entrecruzan ambas previsiones, por un lado «cualesquiera acciones u omisiones que puedan constituir infracciones de derecho de la Unión Europea» —eso sí, acotadas a unos ámbitos establecidos por la Directiva—; y, por otra parte, las que con independencia de los sectores especificados «puedan ser constitutivas de infracción penal administrativa grave o muy grave». En cualquier caso, se pueden formular algunas objeciones y consideraciones respecto al ámbito material de aplicación que se desarrollan a continuación de manera más minuciosa.

3.1. La protección ante la dificultad para inferir el ámbito material de aplicación

Profundizando en el análisis, hay que mencionar que la aparente sencillez para determinar los ámbitos cubiertos por la Ley que se derivan del Derecho de la UE no es tan evidente. Fernández Ramos (2023) se ha encargado de poner de manifiesto la dificultad que conlleva esta operación, porque no basta con observar si el ámbito material relacionado con la infracción está recogido en el artículo 2.1 de la Directiva, sino que en algunos ámbitos concretos debe comprobarse si existe un acto normativo de los enumerados en el Anexo de la Directiva. En otras palabras, no es suficiente que una infracción tenga relación con un campo concreto citado por la Directiva (ej. protección del medioambiente), sino que las infracciones deben

tener su reflejo en un reglamento o directiva de las que se recogen en el citado Anexo[12].

En todo caso, queremos centrar el análisis sobre la dificultad para inferir el ámbito material de aplicación en la ampliación que operó el legislador español. La calificación como infracción grave o muy grave es difícil de inferir con exactitud para personas sin conocimientos jurídicos o, incluso, teniéndolos, es necesario hacer comprobaciones de la legislación vigente. Por ello, no será extraño que algunas personas se abstengan de comunicar información porque no sepan determinar su calificación, o bien, que, al ser desconocedores de estos pormenores hagan comunicaciones y luego tengan problemas para acceder a la protección.

En esta línea, nos podemos preguntar qué ocurrirá con las comunicaciones que se formulen a través de los canales y que correspondan a ámbitos ajenos al Derecho de la UE y que tampoco constituyan infracciones graves o muy graves. Entendemos que, pese a que estas alertas puedan quedar archivadas o inadmitidas, dado que no entrarían en su ámbito material de aplicación —en el canal externo quedarían inadmitidas por aplicación expresa del art. 19.2—, como mínimo, debería mantenerse intacta la garantía de confidencialidad sobre la identidad porque es una de las características intrínsecas del sistema.

Con relación al acceso a la protección, podemos defender en la línea de Piñar Mañas (2020, p. 32) que, siempre que la información se ofrezca de buena fe, debe existir una amplia flexibilidad a la hora de interpretar el ámbito material de aplicación, dado que la redacción de la Ley se focaliza en la posibilidad potencial de que el hecho constituya una infracción grave o muy grave —el artículo 2.1 *b)* utiliza la expresión «puedan ser constitutivas», no que inequívocamente sean constitutivas—. En esta línea, recuperamos la definición que realiza la Directiva de la expresión «información sobre infracciones» (art. 5.2) a la que se refiere como «las sospechas razonables, sobre infracciones reales o potenciales». Más claro aún es el considerando 32 de la Directiva, que se expresa en los siguientes términos: «los denunciantes deben tener derecho a protección en virtud de la presente Directiva si tienen motivos razonables para creer que la información comunicada entra dentro de su ámbito de aplicación». Es una muestra clara de la vocación de apertura y flexibilidad hacia la que se dirige la Directiva respecto al otorgamiento de la protección, que, sin embargo, no queda tan nítida en Ley. Así, en algunos pasajes llegaría a ser contraria a lo dispuesto en la Directiva al excluir de las protecciones lo que no entre dentro de su ámbito material por aplicación del art. 35.2 *d)* —que remite a las causas de inadmisión del art. 18.2 *a)* entre las que se encuentra este supuesto—, aunque previamente se preceptúa como una condición de acceso que se «tengan motivos razonables para pensar que la información (...) entra dentro del ámbito de aplicación de esta Ley» —ex art. 35.1 *a)*—.

De ahí que conviene recordar que, cuando estamos hablando de infracciones graves o muy graves y, siempre que no correspondan al Derecho de la UE, el legislador las ha asumido dentro del ámbito material de aplicación de la Ley sin que exista una obligación de transposición. Por ello, los parámetros de interpretación que ofrece la Directiva pueden no ser aplicables a aquellos ámbitos que cubre voluntariamente el legislador interno. No obstante, la utilización de las mismas expresiones en la Ley, como acciones u omisiones «que puedan ser constitutivas» —ex art. 2.1. *b*)—, nos lleva a entender que se asume la posición expansiva de la Directiva acerca del tipo de información que da acceso a las protecciones, aunque pueda ser exigible que la valoración que realiza el informante sobre la gravedad de los hechos que se comunican sea razonable y no fruto de una actitud irreflexiva.

3.2. La «otra» información para destapar irregularidades y fomentar la integridad

En segundo lugar, que una información no entre dentro del ámbito material de aplicación de la Ley, no debería ser óbice para que nutra las actuaciones, dado que pueden ser la punta de iceberg a partir de la que investigar otras infracciones más graves y cuyo conocimiento es menos accesible. Entendemos de igual modo, que la obtención de información menos relevante, no impedirá que la persona responsable del sistema interno haga las comprobaciones pertinentes sobre su verosimilitud, o que den lugar a procedimientos correctores en el seno de las organizaciones con base en otra normativa aplicable o en la existencia de códigos éticos. Cuestión distinta es que las alertas como tal, deban ser archivadas o inadmitidas a tenor del ámbito material de aplicación de la Ley, sin perjuicio de que se produzca una suerte de efecto memoria entre los gestores de los sistemas de información que pueda ser útil más adelante, por lo que se echa de menos que se hubiera previsto un mecanismo para su rescate y reutilización más adelante, sin perjuicio de las limitaciones que se imponen a la conservación de las comunicaciones[13].

En todo caso, la aspiración mostrada por algunas organizaciones de la sociedad civil y por las Oficinas y Agencias Antifraude autonómicas, era que el ámbito material de aplicación alcanzase a todo tipo de infracciones, pero también a aquellas prácticas que fuesen abusivas y a los comportamientos reprochables por

su colisión con códigos éticos o de conducta que evidenciasen una mala praxis profesional o empresarial. Todo ello bajo la idea de conseguir el máximo rendimiento de los canales en torno a la búsqueda de comportamientos éticos y diligentes y de un cumplimiento íntegro de la legalidad, pero también con la finalidad de perseguir una transposición más acorde a la vocación de la Directiva[14].

Con todo, una solución alternativa o que hubiese mejorado la previsión actual, hubiera conllevado la inclusión expresa de sectores sensibles en los que se puedan producir irregularidades, con independencia de la calificación de la infracción y de su afectación al Derecho de la Unión. Al respecto, podemos traer las reflexiones de Tardío Pato (2022 p. 33) quien defendía la inclusión expresa de todo lo relativo al acceso a la función pública, por tratarse de una materia que se erige en el «primer freno a la corrupción». En su argumentación, insistía en esta idea como primer requisito para una efectiva lucha contra la corrupción: «¿pues, cómo se va a oponer un funcionario a una situación ilegal a la hora de redactar un informe o una propuesta de resolución o de aplicar una resolución de la autoridad política, si ha accedido a la función pública por voluntad personal de esa autoridad política de la que proviene la situación ilegal y si el ascenso o descenso profesional de tal funcionario siguen dependiendo de la voluntad personal de esa autoridad?» (Tardío Pato, 2022 p. 34).

3.3. Información excluida y su relación con la responsabilidad penal

Con relación a la exclusión de ámbitos concretos. La Ley descarta la protección ante comunicaciones de información clasificada, o que pudiese estar sometida al secreto que deben guardar los profesionales de la medicina y de la abogacía, el secreto de las deliberaciones judiciales, o que está afectada por el deber de confidencialidad de las de las Fuerzas y Cuerpos de Seguridad «en el ámbito de sus actuaciones» (art. 2.4). Del mismo modo, tampoco se aplica la Ley para las informaciones sobre infracciones respecto a «procedimientos de contratación que contengan información clasificada o que hayan sido declarados secretos o reservados, o aquellos cuya ejecución deba ir acompañada de medidas de seguridad especiales conforme a la legislación vigente, o en los que lo exija la protección de intereses esenciales para la seguridad del Estado» (art. 2.5).

Sin ánimo de querer centrar el análisis en esta cuestión, es necesario hacer un apunte relevante sobre el alcance de estas exclusiones, dado que pueden existir muchos otros supuestos previstos en el ordenamiento jurídico que obligan a guardar secreto y que no quedan excluidos expresamente de la protección por la Ley. En otras palabras, al no hacer referencia a otros supuestos distintos, en teoría darían acceso a la protección, pero no en toda su extensión como a continuación se explica.

El artículo 38 expresa entre las medidas de protección que los alertadores «no incurrirán en responsabilidad de ningún tipo en relación con dicha comunicación o revelación pública», aunque esta previsión «no afectará a las responsabilidades de carácter penal» (art. 38.1). Se observa que esta cláusula abierta del artículo 38.1, salvo para la responsabilidad de carácter penal, choca frontalmente con su apartado 5, en el que se reitera la exención de responsabilidad en los procesos judiciales en general, citando particularmente aquellos que tengan relación con la vulneración de secreto o por relevación de secretos empresariales. Esto nos origina más incógnitas que certidumbre, porque la Ley no viene acompañada de una modificación del Código Penal (CP) que nos aclare si hay o no responsabilidad penal de los alertadores ante la posible comisión de delitos relacionados con la revelación de secretos. Al respecto, entiendo que, para la exención o atenuación de la responsabilidad penal, hubiera sido necesaria una modificación del Código Penal y no una mera declaración de intenciones como parece formular este apartado 5 del artículo 38. Por ello, existirá información excluida de la protección en términos de responsabilidad penal cuando su mera comunicación constituya un delito, como tampoco la hay si la información ha sido obtenida mediante la comisión de un delito (ex art. 38.2)[15]. Si la intención del legislador hubiera sido otra, se debería haber operado una modificación del Código Penal[16].

3.4. Regímenes especiales y concurrencia de la regulación

La última objeción que hacemos constar, tiene relación con la existencia de sectores excluidos y con la aplicación concurrente de normativa. El artículo 2.6 prevé la existencia de regímenes específicos para las alertas en determinados sectores, cuya pervivencia suele ser una fuente de confusión y conflicto, como bien se ha mostrado en el ámbito del derecho de acceso a la información pública, en particular, sobre la controversia para apreciar cuando estamos ante un régimen específico y cuando no. La Ley preceptúa que, en su caso, se rigen por su propia normativa las materias incluidas en la parte II del Anexo de la Directiva, es decir, algunas parcelas de ámbitos concretos relativos a servicios financieros, prevención del blanqueo de capitales y financia-

ción del terrorismo, seguridad del transporte (sucesos de aviación civil, responsabilidades del Estado sobre trabajo marítimo, control de buques) y protección del medio ambiente (seguridad de operaciones relativas al petróleo y al gas mar adentro). Se trata de regulaciones muy concretas que requieren conocer el estado de la normativa y su alcance para observar si es de aplicación la regulación de la Ley.

En último término y sobre estos regímenes específicos, se podría defender que lo contenido en la Ley que ahora nos ocupa, debe ser de aplicación cuando existan lagunas en esa regulación específica en aspectos que no estén previstos, ni en sus normas reguladoras, ni en las normas europeas de las que traen causa muchas de ellas. Al respecto, es necesario recordar que el artículo 3.1 de la Directiva indicaba que ésta sería aplicable «en la medida en que un asunto no se rija obligatoriamente» por los actos sectoriales de la Unión relativos al precitado Anexo II.

Adicionalmente, hay que señalar que las protecciones de la Ley son concurrentes con legislación sobre alertas de infracciones del Derecho laboral en materia de seguridad y salud en el trabajo (art. 2.3), y que, en todo caso, «no excluirá la aplicación de las normas relativas al proceso penal, incluyendo las diligencias de investigación» (art. 2.2).

3.5. La información para dar pistas sobre el ámbito material de aplicación

Con todo, y pese a todas las excepciones totales o parciales que pueden existir, la reflexión es que el ámbito material alcanza un vasto campo, tanto derivado del derecho de la Unión, por la afectación a sus intereses financieros o por su incidencia en el mercado interior, como por todo lo que pueda ser constitutivo de infracción penal o administrativa (grave o muy grave).

Aun así, existen vías de escape, por lo que adquiere una singular relevancia la información que se facilite a los potenciales alertadores sobre el régimen aplicable en cada organización. La Ley obliga a proporcionar «información adecuada de forma clara y fácilmente accesible, sobre el uso de todo canal interno de información que hayan implantado, así como sobre los principios esenciales del procedimiento de gestión», debiendo constar en una sección de su página web si dispusieran de ella (art. 25). Pese a este precepto, se echa de menos que las obligaciones de información hubiesen sido más concisas a imitación de lo que impone el artículo 25 *a)* para las autoridades que gestionan el canal externo, que deberán publicar información sobre las condiciones para acogerse a la protección.

De todas formas, sería deseable que los sujetos obligados incluyan de manera generalizada y con cierto grado de detalle, el tipo de infracciones asociadas a su sector de actividad y el régimen jurídico específico que sea de aplicación. En las empresas privadas parece más evidente que la información se termine modulando en función del sector de actividad, y de sus productos y servicios. De igual manera, algo similar podrá ocurrir en las entidades públicas cuyas funciones sean muy especializadas y puedan delimitar el tipo de irregularidades a comunicar. Sin embargo, no es de esperar que suceda lo mismo ante las administraciones públicas territoriales cuyas competencias se proyectan de manera generalizada en una multitud de ámbitos y en los que sea más habitual la existencia de múltiples excepciones por ser de aplicación regímenes especiales. Así, uno de los retos de los sistemas de alertas consiste en informar bien y claramente sobre el tipo de infracciones y régimen al que se sujetan sus canales de alerta.

4. Ámbito personal de aplicación: delimitación, nexo profesional, personas jurídicas y vías de escape

Como ya se ha avanzado, los alertadores son los protagonistas del sistema de protección, pero bajo la definición de la Ley, hemos de advertir que el informante no es cualquier persona, sino quien obtiene la información en el marco de su actividad laboral o profesional; al igual que, tampoco, hay una correspondencia exclusiva de la figura del alertador con la del protegido. A continuación, tratamos con más detalle ambas cuestiones, junto a algunas consideraciones sobre la extensión del concepto de informante y del protegido.

4.1. Personas que alertan o informan

El texto define en su artículo 3 a las personas informantes como aquellos «que trabajen en el sector privado o público y que hayan obtenido información sobre infracciones en un contexto laboral o profesional». En una primera lectura de este fragmento, queda clara la orientación hacia un ámbito de trabajo, porque es donde cobran sentido el tipo de protecciones que

Núm. 24 zk./2023. Págs. 70-98 or.
ISSN: 2173-6405 e-ISSN: 2531-2103

prevé la Ley, en las que el informante es susceptible de quedar más expuesto a represalias de terceras personas de su organización.

Más aún, la Ley supera conceptos como el de trabajador por cuenta ajena o el de empleado público. Así, se alude al ámbito «profesional» y se atribuye la cualidad de informante a los autónomos, a «los accionistas, partícipes y personas pertenecientes al órgano de administración, dirección o supervisión de una empresa, incluidos los miembros no ejecutivos», y a aquellos que trabajen «para o bajo la supervisión y la dirección de contratistas, subcontratistas y proveedores». Además, el texto no queda ahí, porque incorpora a quienes obtuviesen la información debido a una relación de trabajo finalizada, a voluntarios, becarios, trabajadores en periodos de formación, así como a aquellos que se encuentran inmersos en un proceso de selección o negociación precontractual. Es decir, se asume una definición extensiva del informante como persona que obtiene una información en un entorno profesional, aunque estas previsiones no supongan una novedad porque se ciñen a los supuestos que ya establecía la Directiva.

Cabe señalar que la enumeración mencionada se precede de la expresión «comprendiendo en todo caso», lo que conlleva que no estemos ante una lista cerrada, sino que, como mínimo, incluirá a esas diferentes figuras que se explicitan. Esto abre la puerta a que perfiles distintos entren en su ámbito de aplicación, siempre que se asocie a lo laboral o lo profesional, y que en el ámbito público da lugar a una variedad muy amplia de figuras que pueden actuar como posibles informantes.

Es más, debemos tener en consideración que no se exige que la información obtenida sea estrictamente sobre la propia organización en la que se trabaja, aunque pueda ser el caso más frecuente. De hecho, la Directiva definía la información sobre infracciones en su artículo 5.1 como aquella referida a las que «puedan producirse en la organización en la que trabaje o haya trabajado el denunciante o en otra organización con la que el denunciante esté o haya estado en contacto con motivo de su trabajo». Por esta razón, un conocimiento adquirido en el desarrollo de la actividad laboral o profesional sobre terceros, podría provocar el acceso a protecciones si tuviera sentido que la alerta provocase un retorno negativo a la persona informante.

En este punto, conviene aclarar que en el artículo 36.2 enumera, a modo de ejemplo, tanto las represalias más grotescas —separación del puesto de trabajo— como supuestos más perspicaces, pero que, de todas maneras, abarcarán a cualquier acto u omisión que «de forma directa o indirecta, supongan un trato desfavorable» [17], por lo que se abre la puerta a considerar como tales a una variedad muy amplia de circunstancias que se pueden producir más allá de una relación laboral directa.

4.2. **Personas objeto de protección**

En todo caso, el objeto de protección no sólo será la persona informante, sino también otros sujetos que puedan tener relación o contacto con él durante el proceso de comunicación de infracciones. La Ley incluye dentro de la protección a los «representantes legales de las personas trabajadoras en el ejercicio de sus funciones de asesoramiento y apoyo al informante» (art. 3.3) y también a personas físicas y jurídicas relacionadas con él (art. 3.4). Entre las personas físicas quedarían protegidas —en lo que sea aplicable— aquellas que asistan al alertador en su organización durante el proceso y, también, las que estén relacionadas con el informante y que puedan sufrir represalias, citando compañeros de trabajo o familiares a modo de ejemplo. Sobre las personas jurídicas, la protección se proyecta «para las que trabaje o con las que mantenga cualquier otro tipo de relación en un contexto laboral o en las que ostente una participación significativa». Como afirma Parajó Calvo (2022), de este modo se establecen dos niveles de aplicación subjetiva de la Ley, una plena para las personas informantes —serán informantes y estarán protegidos—, y una parcial para quienes forman parte de su entorno o le prestan asistencia —no serán informantes, pero podrán estar protegidos—.

Además, la persona afectada también entra dentro de las figuras protegidas, es decir, aquellas personas que se mencionan en las comunicaciones como posibles responsables de las infracciones. Que no sean el objeto en el que queremos centrar la atención, no les resta importancia como sujeto que también es necesario salvaguardar de alertas infundadas o falsas y, por ello, gozarán «durante la tramitación del expediente» de la «misma» protección que los informantes (art. 39). A esta equiparación se añade la referencia a la necesidad de garantizar la presunción de inocencia, el derecho de defensa y de acceso al expediente bajo las condiciones que establece la Ley (art. 39). Esta es de las previsiones más fuertes que constan sobre los afectados, ya que esta figura está huérfana de un tratamiento extenso en la Ley. Sin embargo, su acceso a las protecciones «durante la tramitación del expediente» nos lleva a preguntarnos sobre su alcance y las posibles contradicciones que se pueden pro-

ducir. Con la protección se pretende evitar que su mero señalamiento les provoque perjuicios, pero puede generar un contrasentido al dificultar que se aparte de manera preventiva a un afectado, cuando haya indicios clarísimos de la comisión de infracciones muy graves sobre las que todavía no se haya terminado dicha tramitación.

4.3. **La formulación de alertas por sujetos ajenos a una vinculación laboral o profesional**

De lo visto hasta aquí, sobre el concepto «informante» no se puede destacar nada sustantivo que la Directiva no hubiese previsto ya con relación a esa vinculación con el ámbito profesional y de trabajo. Una alternativa podría haber sido incluir a las personas que denunciasen infracciones, con independencia de haber conocido la información en el marco de una relación laboral o profesional y otorgarles protección en lo que fuese aplicable, extremo que no se contempla, aunque no siempre con una meridiana claridad.

a) *Argumentos para abrir las alertas en los canales internos*

En cualquier caso, podríamos preguntarnos si tiene sentido que alguien que no trabaja o lo haya hecho en una organización debería poder emitir alertas a través de un canal interno. Entiendo que sí por los argumentos que a continuación se detallan.

En primer lugar, hay colectivos a quienes hubiera sido muy razonable incluir, como puede suceder con los usuarios de servicios públicos[18]. Piénsese en una persona que está en lista de espera para una operación y le llega información sobre infracciones cometidas en el establecimiento hospitalario. Podríamos discutir, incluso, si es una información conocida en un contexto laboral o profesional. En todo caso, todavía se hubiese podido dar un giro de tuerca más para facilitar las alertas y amparar sin ambages a quienes comunican infracciones sin ser informantes en los términos del artículo 3 de la Ley. Como ya defendí en su momento (Sierra Rodríguez, 2020a), la opción de abrir los canales de denuncia a cualquier persona, y singularmente los externos, permitiría obtener mucha más información valiosa, aunque ello conllevase una mayor carga de trabajo para cribar la que tuviese verosimilitud.

En segundo lugar, no sería tan extraño la necesidad de aplicar algunas de las protecciones previstas a personas sin vinculación laboral o profesional. Siguiendo el ejemplo mencionado, podría suceder que alguien postergase el llamamiento de un paciente que está en lista de espera en represalia por haber formulado una alerta, o más sencillamente, que el afectado denuncie al alertador por difamación.

b) *Las dudas sobre la admisión y seguimiento de alertas en el canal externo*

Estamos haciendo alusión al canal interno por la relevancia que le otorgan la Directiva y la Ley para que constituya la vía preferente de comunicación de información, pero en el caso del canal externo se sigue manteniendo esta exclusión de quienes no estén conectados con un entorno laboral o profesional —al menos en apariencia—.

En mi opinión, el canal externo se trata del lugar idóneo en el que podría haberse depositado la recepción de información proveniente de cualquier ciudadano o ciudadana ajeno/a a la organización en la que se producen los hechos, a imitación de cómo se ha venido haciendo en algunas agencias y oficinas antifraude autonómicas y municipales.

Sobre esta cuestión, podría llevar a equívoco el artículo 16 de la Ley sobre el canal externo, porque expresa que «toda persona física podrá informar» sin hacer más delimitaciones que las referidas a las «acciones u omisiones incluidas en el ámbito de aplicación de esta ley». Esto nos conduce a pensar que el legislador había optado por acoger el criterio de apertura a la ciudadanía. Sin embargo, el preámbulo de la Ley nos ayuda a interpretar que se mantiene vigente el condicionamiento, porque se trata de un «canal externo ante el que podrán informar las personas físicas a las que se refiere el artículo 3 de la ley».

Sin embargo, hay pocas barreras que impidan que también puedan informar otras personas distintas. Durante el primer paso del análisis de la información recibida en el canal externo, no se contempla un mecanismo de exclusión con base en el tipo de relación que deba tener quien envía la alerta con un ámbito profesional o laboral en el que haya conocido la información. Así, las causas de inadmisión previstas en el artículo 18.2 *a)* sí prevén su aplicación cuando la información no entre dentro del ámbito material, pero nada se dice sobre el cumplimiento de los requisitos sobre el ámbito personal del artículo 3.

Es más, dada la amplia variedad de circunstancias y perfiles que se contemplan en torno a la figura del informante, tampoco sería fácil de delimitar, a priori, si una información se ha obtenido en un contexto profesional o no, salvo que el alertador haya dejado pa-

tente que es ajeno a este supuesto. Entendemos que las alertas de cualquier persona se podrán canalizar por el canal externo y que se les dará seguimiento en las mismas condiciones, porque no existe una causa de inadmisión expresa, aunque esa persona pueda quedar excluida de las protecciones en caso de pretender su acceso a ellas.

De manera consciente o inconsciente, el legislador viene a abrir esta ventana de oportunidad que se verá materializada o no, en función de la implantación concreta que se haga de los canales, en los que eventualmente se pueda controlar si el alertador se corresponde con los supuestos que permitan calificarlo como informante a tenor de lo establecido en la Ley.

En todo caso, por la orientación de la norma, se tienden a minorar las posibilidades de colaboración ciudadana sobre las que podían existir amplias expectativas (Cerrillo i Martínez, 2018). De hecho, tampoco se han incluido otros perfiles como podrían ser los intermediarios o activistas que desempeñen un papel similar al de los representantes de los trabajadores, pero trasladado al ámbito del acompañamiento desde fuera de la organización[19].

A lo sumo, será necesario que las autoridades independientes de protección del informante terminen de aclarar hasta donde se puede extender la calificación como informante o de acceder a las protecciones y prestaciones de apoyo. Sobre estas últimas, se reitera que para acceder a ellas (art. 35.1 y 2), se exige el cumplimiento de los requisitos sobre la información del artículo 2, pero se habla únicamente de quien comunique o revele este tipo de información, sin circunscribirla expresamente a quienes tengan la calificación de informante y sin hacer mención a aquellos que pueden acceder a la protección por su relación con el informante (ex art. 3.4). Por tanto, podríamos llegar a entender que existe una vía abierta para que las protecciones sean aplicables a otros colectivos distintos[20].

Con todo, sería de esperar que las autoridades independientes adopten un posicionamiento equivalente a la actitud proacceso que, en el ámbito de la transparencia, han mostrado los Consejos y Comisionados de la Transparencia y que se ha visto respaldada por los tribunales. Además, como recuerda Piñar Mañas (2020 p. 114) hay cierta inercia comunitaria que podría influenciar esta deriva, considerando que, tanto la Comisión Europea, como el Tribunal de Justicia de la Unión Europea «suelen ser extremadamente generosos al interpretar normas europeas de protección, que pretenden garantizar la efectiva aplicación del ordenamiento europeo y por ende de los ordenamientos nacionales».

4.4. La otra puerta de atrás para hacer llegar alertas por la ciudadanía

Una mayor profundización nos lleva a observar que la configuración normativa que se deduce para los canales internos y externo, provocará supuestos en los que se abre una puerta de atrás adicional por la que se pueden colar alertas sin cumplir los requisitos que se establecen para la figura del informante.

Esto sucede porque el canal interno, siempre que esté bien diseñado, deberá ser accesible desde fuera de la organización, dado que los extrabajadores, candidatos a puestos de trabajo u otras figuras recogidas expresamente en la Ley como informadores, no tienen por qué tener acceso a los sistemas informáticos o espacios físicos de la empresa u organización, lo que obliga a que sean accesibles desde fuera y sin restricciones.

Aun así, se podría pensar en que es posible aplicar el filtro relativo a la existencia de una relación vigente o anterior, pero hay que recordar que los sistemas deben permitir el anonimato (art. 7.3). En estos casos, se dificulta cualquier control previo sobre el tipo de vinculación, e incluso posterior, siempre que no se termine desvelando la identidad. Al respecto es conveniente tener muy clara la diferencia entre confidencialidad y anonimato. Mientras la primera está relacionada con la custodia y la reserva de la identidad de una persona que, en algún momento, se ha dado a conocer o ha consignado sus datos; la segunda, conlleva que no haya datos identificativos de ningún tipo y que ni siquiera se pueda determinar su identidad, lo contrario impediría hablar de la garantía de anonimato.

Esta conjunción de factores —accesibilidad desde fuera y anonimato— provoca que se puedan formular alertas por cualquier persona, siempre que, como hemos dicho, se mantenga en el anonimato, por lo que consecuentemente no podrá acogerse a las protecciones, porque si revela su identidad quedaría patente que no se encuentra dentro del ámbito de aplicación personal del precitado artículo 3.

4.5. Sobre la extensión de las protecciones a las personas jurídicas

En último término se subraya que la cualidad de informante está circunscrita a las personas físicas, aunque no impide que actúe como alertador una persona física con vocación de hacerlo en representación de una entidad. Bajo este marco, la persona jurídica no podrá tener la cualidad de informante, pero como se ha dicho, en algunos casos, podría gozar de protecciones. Esto es así porque el artículo 3.4 *c)* lo prevé

para las «personas jurídicas, para las que trabaje o con las que [el informante] mantenga cualquier otro tipo de relación en un contexto laboral o en las que ostente una participación significativa» [21]. Una primera lectura de este artículo, nos lleva a mantener que las acciones de regreso indirectas que sufran las organizaciones con las que está vinculado el informante estarán amparadas en lo que sea aplicable del régimen de protección a las personas jurídicas. El considerando 41 de la Directiva ejemplifica algunas de ellas como la «denegación de prestación de servicios, la inclusión en listas negras o el boicot a su actividad empresarial».

Para que aplique este régimen se exige, eso sí, que el alertador tenga algún tipo de vinculación laboral o participación significativa en esa entidad en términos de capital o derechos de voto que le lleven a tener capacidad de influencia —art. 3.4 *c)*—. Esta articulación permitiría el amparo a una empresa subcontratista en cuyo capital participa el informante, y aunque la redacción empleada parece estar orientada a sociedades mercantiles, para nada es descartable que la interpretación de este precepto acoja a asociaciones, sindicatos y a otras organizaciones, siempre que los informantes tengan un cargo directivo o posean una capacidad de influencia en su gobierno. De hecho, la expresión relativa a mantener «cualquier otro tipo de relación en un contexto laboral», sería susceptible de extender más el tipo de personas jurídicas objeto de protección a aquellas en las que participa el alertador con una colaboración que sea asimilable a un contexto laboral.

5. El sistema interno de información

Examinado el ámbito material y personal de aplicación, nos adentramos en lo que se viene a denominar como sistema interno de información, al que la Ley dedica su Título II (arts. 4 a 15), con unas disposiciones comunes (arts. 4-9) y unas previsiones diferenciadas para el sector privado (arts. 10-12) y para el público (arts. 13-15).

Aunque no se define qué debe entenderse por un sistema de información, del articulado se puede extraer que estamos ante una serie de piezas entrelazadas e interdependientes para el funcionamiento eficaz del esquema de alertas y de protección. En concreto, sus principales elementos serían los canales internos de recepción de información; las políticas y procedimientos de gestión de información y de protección de los alertadores; y los responsables de gestionar el sistema. En todo caso, sus rasgos básicos se extraen del artículo 5 entre los que destaca su diseño y gestión segura, sin accesos no autorizados y garantizando la confidencialidad sobre las identidades y las actuaciones que se llevan a cabo —ex art. 5.2 *b)*—; y garantizando que las alertas sean tratadas de manera efectiva «con el objetivo de que el primero en conocer la posible irregularidad sea la propia entidad u organismo» —ex art. 5.2 *e)*—.

5.1. Los sujetos obligados a disponer de un sistema de información

La disposición de este sistema es obligatoria para todo el sector público con independencia de su número de trabajadores (art. 13.1) y se amplía a «los órganos constitucionales, los de relevancia constitucional e instituciones autonómicas análogas a los anteriores» (art. 13.2). De este modo, quedan obligados a disponer de este sistema todas las administraciones públicas, sus organismos y entidades dependientes, universidades, fundaciones, sociedades participadas, corporaciones públicas, entre otras[22]. Con relación a lo dispuesto en la Directiva (art. 8.9), existía libertad para que el legislador eximiese a los municipios de menos de 10.000 habitantes o con menos de 50 trabajadores, algo que no se ha contemplado finalmente en el ámbito público.

En el sector privado se utiliza la ratio del tamaño de plantilla para la imposición de obligaciones, siendo aplicable con carácter general a todas las personas físicas o jurídicas con 50 o más trabajadores (art. 10)[23]. Hay una serie de supuestos en el sector privado en los que es obligatorio disponer de este sistema con independencia de su número de efectivos, afectando a «los partidos políticos, los sindicatos, las organizaciones empresariales y las fundaciones creadas por unos y otros, siempre que reciban o gestionen fondos públicos» —art. 10.1 *c)*—; así como a las personas jurídicas que actúen en algunos sectores sensibles con normativa específica en la materia, en cuyo caso, la Ley actuará con carácter supletorio —art. 10.2 *b)*—[24]. No se contemplan en la Ley otros supuestos que se podrían haber incluido con independencia del tamaño de plantilla de la organización, en supuestos como superar un determinado umbral económico de recepción de subvenciones o contratos públicos, o tratarse de entidades concesionarias de servicios esenciales para la comunidad.

Con todo, es relevante que las organizaciones que desempeñan funciones constitucionales y que es-

tán insertas en el funcionamiento de nuestro sistema democrático deban tener un sistema interno de información. Los partidos políticos por su relación con el ámbito público y por el alcance que tienen los casos de corrupción política, deberán cumplir con todas las obligaciones con independencia de su tamaño de plantilla, y aunque las grandes formaciones políticas ya estarían obligadas por superar los 50 trabajadores, con esta previsión se incorporan los pequeños partidos de menor tamaño que puedan operar en los ámbitos locales en los que también han aflorado sonados casos de corrupción urbanística. En consecuencia, habrá más posibilidades de cercar los casos de corrupción política que implican a dos o más partes a través de sus respectivos sistemas de información (empresas, administración pública y/o partidos políticos)[25]. También se observa acertada la formulación abierta sobre el alcance de la obligación a los órganos de relevancia constitucional y equivalentes autonómicos, de manera que una enumeración cerrada no dé lugar a omisiones, como sucedía en el caso de la Ley 19/2013, de 9 de diciembre, de Transparencia, Acceso a la Información Pública y Buen Gobierno con la Fiscalía General del Estado porque no se encontraba entre los sujetos obligados.

5.2. **Factores para el cumplimiento normativo: idoneidad, plazos, recurso y orientaciones**

Antes de abordar los elementos básicos del sistema interno, conviene incidir en algunos aspectos que van a condicionar el grado de esfuerzo y posibilidades para su adecuada puesta en marcha. Haremos alusión a su idoneidad, a los plazos para su implantación, a las posibilidades de adaptar los sistemas actuales, compartir recursos o externalizar su gestión, así como respecto a la necesidad de modelos y recomendaciones ante las imprecisiones de la Ley.

a) *La idoneidad más allá de la obligación legal*

Hay una serie de consideraciones que pueden actuar como palanca para que haya un mayor interés de las organizaciones en disponer de sistemas internos atractivos para los potenciales informantes, sin que la única motivación sea dar cumplimiento a lo previsto en la Ley.

Como mencionaba Lozano Cutanda (2020), tal y como está configurado el esquema de canales, por razones prácticas, a las organizaciones les conviene que no se acuda directamente a las vías alternativas como son el canal externo y la revelación pública, de modo que puedan «reaccionar frente a las denuncias antes de que se hagan públicas, lo que facilitará prevenir daños reputacionales y riesgos financieros».

Desde mi punto de vista y pese a lo que diré más adelante sobre los riesgos de estos canales internos, su principal idoneidad radica en que una alerta temprana puede cortar de raíz algunos comportamientos que, de no pararse a tiempo, terminen constituyendo infracciones más graves, ilícitos penales o causen daños o consecuencias irremediables a otras personas o a la organización.

Además, para el sector privado no podemos olvidar que, con la nueva Ley, difícilmente se dará por cumplida la previsión que permite evitar la responsabilidad penal de las personas jurídicas del artículo 31 bis CP si no se dispone del sistema interno. Como remarca González Granda (2021 p. 374), en el Código Penal no se contempla expresamente que se deba implantar un canal de denuncias, pero sí un sistema sancionador adecuado y la obligación de informar sobre los riesgos e incumplimientos al órgano encargado de su modelo de prevención, lo que «exige un sistema adecuado de detección de las infracciones» y que se ayude a «denunciar las irregularidades internas», por lo que «ha de entenderse que debe implantar un canal de denuncias. Y así lo interpreta la doctrina, jurisprudencia y los estándares ISO».

b) *Un periodo de implantación insuficiente*

Una previsión a tener cuenta es la regla general establecida para los sistemas internos, que deberán estar operativos en el plazo de tres meses desde la entrada en vigor de la Ley (Disposición Transitoria 2.ª). En otras palabras, en junio de 2023 la generalidad de las organizaciones debería contar con un sistema listo para funcionar con todos sus elementos: canales, procedimiento, responsable designado, etc. No obstante, se amplía hasta el 1 de diciembre de 2023 para entidades de menor envergadura: en el sector privado para los sujetos obligados entre 50 y 249 trabajadores, y en el sector público para los municipios con menos de diez mil habitantes.

El plazo general de tres meses es tan corto, que nos lleva a pensar sobre la inviabilidad de cumplir muchas de las especificaciones de estos sistemas[26], particularmente en el ámbito público cuando sea necesario activar procedimientos que llevan meses: de contratación pública para dotar a los canales de las características que se exigen, para la designación del responsable del sistema y del personal que deba desarrollar funciones, entre otros. Más aún, se impide una valoración y planificación sosegada, actividad que debería ser el paso previo a la adopción de un modelo

de gestión de denuncias (Gutiérrez Rodríguez, 2022 p. 85)[27]. Se debe tener en cuenta, además, que la implantación de estos sistemas no puede tratarse de una decisión directa de los órganos de administración o gobierno de los sujetos obligados, sino que se debe hacer una consulta previa a la representación de los trabajadores (art. 5.1).

En suma, la reflexión que quiero remarcar es que una deficiente puesta en marcha por hacerlo deprisa y corriendo, puede dar lugar a brechas de seguridad, a la ruptura de la confidencialidad, a la falta de seguimiento de las alertas o a otras patologías, con el riesgo de provocar que, de manera temprana, se frustren las expectativas de quienes los usen y se genere un boca a boca negativo y una actitud recelosa que no aliente su utilización.

c) *La posibilidad de adaptación*

En cualquier caso, se podrán aprovechar los esfuerzos ya realizados en esta materia. A tal efecto se expresa la Disposición Transitoria 1.ª al indicar que los sistemas preexistentes podrán servir para el cumplimiento de las obligaciones que se imponen, siempre que cumplan con los requerimientos de la Ley.

Podríamos divagar si esto coadyuvaría a llegar en mejores condiciones al plazo marcado al existir comunidades autónomas y algunos municipios que ya habían avanzado en esta materia. Del mismo modo, también existen figuras y sistemas asimilables, tanto en el sector público, como en el privado, que venían desarrollando funciones parecidas (nótese particularmente los sistemas de compliance en las empresas para evitar la responsabilidad penal).

No obstante, las experiencias autonómicas y municipales son pocas y la diversidad de fórmulas preexistentes es patente y difiere de lo establecido en la Ley. Además, como menciona Villoria Mendieta (2021b p. 23 y 24) en el sector público apenas hay verdaderos sistemas de gestión de la integridad; mientras que los canales de denuncia interna solo han empezado a generalizarse en las sociedades mercantiles públicas por su afectación a la responsabilidad penal de las personas jurídicas del art. 31 *quinquies* del Código Penal (Sáez Hidalgo. 2021)[28]. Más aún, podemos preguntarnos si los tradicionales órganos de intervención y control interno en las administraciones públicas son los más idóneos para asumir estas funciones, dada la cultura y dinámica de trabajo excesivamente formalista cuya inoperancia es, precisamente, la que justifica más aún estos cambios normativos. Consecuentemente y ante los casos de corrupción —tanto de los conocidos como de los que han pasado más desapercibidos—, surge la incógnita respecto a si el número de funcionarios que han perdido su condición responde a la realidad de la comisión de infracciones en las administraciones públicas.

d) *Compartir y externalizar recursos*

En ambos casos —sector público y privado— se permite que los sujetos obligados compartan medios cuando se trate de entidades de pequeño tamaño (arts. 12 y 14). Los supuestos en el sector público quedan condicionados a que se trate de municipios con menos de 10.000 habitantes, en cuyo caso podrán compartir recursos entre sí o con otras administraciones públicas del territorio de su comunidad autónoma (art. 14.1); o de «entidades del sector público con personalidad jurídica propia que estén vinculadas o dependan de órganos de las administraciones territoriales y cuenten con menos de 50 trabajadores» que los podrán compartir con su administración de adscripción (art. 14.2). Bajo estos dos supuestos podrán compartir recursos siempre que se garantice que los respectivos canales y sistemas aparezcan diferenciados entre sí (ex art. 14.3).

La previsión para compartir medios era necesaria para los municipios más pequeños —la Directiva daba margen para ello—, dado que la continua imposición de obligaciones por muy loables o necesarias que sean, quedan condenadas a su incumplimiento si no se acompañan de medios o se ofrecen alternativas para facilitar su observancia.

Como veremos a continuación, los canales de recepción de alertas conllevan una alta complejidad técnica porque ya no se trata de poner un buzón o habilitar un correo electrónico, sino que hay exigencias importantes respecto a seguridad, confidencialidad y registro de la información que precisa de personal especializado y de medios técnicos adecuados de los que no todas las organizaciones disponen. Pese a la voluntad de compartir recursos, la diversidad de la administración local de nuestro país nos lleva a pensar que muchos ayuntamientos precisarán apoyo para el cumplimiento de estas obligaciones. A este respecto Iglesias Rey (2022 p. 184) entiende que será necesario que las comunidades autónomas y las diputaciones provinciales articulen mecanismos de subvenciones u otros que permitan dar asistencia a las entidades de tamaño reducido, algo para lo que seguiría faltando un mayor plazo que el otorgado por la Ley.

En todo caso, la otra alternativa para el sector público ante la premura de los plazos es acudir a un tercero externo, aunque para ello se precisa justificar la insuficiencia de medios (art. 15). Como subrayaba Sáez Hidalgo (2021) para los municipios se podría hablar, incluso, de su conveniencia en términos de oportunidad

y eficacia, dado que la relación en términos jerárquicos, económicos y funcionales que son propias de la administración pública «se intensifica aún más cuando sus dimensiones son reducidas, donde las relaciones personales son mucho más intensas, todo lo cual podría poner en peligro éxito de la investigación (destrucción de pruebas..) o al propio denunciante (vulneración de la confidencialidad, posibles represalias, etc.)». No obstante, es relevante subrayar que para el sector público y a diferencia de lo que ocurre cuando se comparten recursos, la gestión de un tercero externo debe limitarse al «procedimiento para la recepción de las informaciones sobre infracciones» que «en todo caso, tendrá carácter exclusivamente instrumental» (art. 15).

e) *La carencia de orientaciones ante las imprecisiones de la Ley*

Finalmente, como factor para el cumplimiento óptimo de las disposiciones de la Ley y ante el contexto señalado sobre sus imprecisiones, cobran singular trascendencia las recomendaciones u orientaciones para la implementación de estos sistemas. Sin embargo, no parece que vayamos a tener una autoridad estatal en funcionamiento de manera rápida, lo que deja a los sujetos obligados sin la posibilidad de dirigirse a una entidad de referencia, más allá de lo que puedan obtener de consultoras privadas, de los servicios de intervención o asimilables que hayan estado trabajando estas materias, o de las oficinas y agencias antifraude que existen en algunos territorios.

El artículo 43 autoriza la creación de la autoridad estatal, mientras que la Disposición Final 11 fija el plazo máximo de un año para la aprobación de su Estatuto, de ahí que, parece que serán necesarios muchos meses para que la autoridad cuente con todo lo necesario como para hacer recomendaciones u ofrecer orientaciones. Lo mismo podemos predicar respecto a las autoridades autonómicas en aquellas comunidades autónomas en las que no existen y que deberán ser determinadas a través de instrumentos jurídicos que no siempre son ágiles.

6. El canal interno

La primera de las piezas de este sistema que analizamos con más detalle es el canal interno. Éste se configura en la Ley como algo que va más allá de un buzón, porque sobre los canales se fijan muchos requerimientos que parten de la necesidad de garantizar su seguridad y la confidencialidad del informante y de las comunicaciones (art. 7). A continuación, abordamos su número y modalidad, sus condicionantes técnicos y su posible integración para recibir otro tipo de comunicaciones.

6.1. Número de canales y modalidad

La redacción del artículo 7.2 dificulta conocer si se exige uno o varios canales y cuál debe ser su modalidad concreta porque utiliza formulaciones ambiguas respecto al tipo de comunicaciones que pueden formularse: «por escrito o verbalmente, o de las dos formas». Es decir, bajo esta redacción obliga solo a disponer de una de las tres opciones a criterio del sujeto obligado, extremo que nos suscita muchas incertidumbres en el momento en que, eventualmente, se opte por la unimodalidad —solo por escrito o solo verbalmente—, con las limitaciones que ello conlleva para articular plenamente las características que se exigen y para ofrecer versatilidad a los potenciales alertadores.

En todo caso, la responsabilidad de esta ambigüedad es del legislador europeo, porque la Directiva utiliza la misma expresión para las denuncias internas (art. 9.2 Directiva); mientras que para el canal externo el mandato es claro al indicar que permitirán denunciar «por escrito y verbalmente» (art. 12.2 Directiva)[29]. Para una mayor nitidez, hay que acudir al considerando 53 de la Directiva que afirma: «Siempre que se garantice la confidencialidad de la identidad del denunciante, corresponde a cada entidad jurídica individual del sector privado y público definir el tipo de canales de denuncia que se hayan de establecer».

Así, la Ley viene a enumerar un repertorio de las formas de recepción bajo una redacción barroca que obstaculiza conocer cuáles son las mínimas que se exigen en cada modalidad. Entre las fórmulas escritas se cita el correo postal y los medios electrónicos. Entre las verbales, la vía telefónica y los sistemas de mensajería de voz. Preceptúa que, en todo caso, se podrá ofrecer la información mediante una reunión presencial si así lo solicita el informante (art. 7.2).

Esto nos lleva a la inevitable conclusión de que el legislador español se ha limitado a transponer la Directiva en todos sus términos y nos hace preguntarnos si habrá sujetos obligados que se ceñirán a poner una única vía de recepción, aunque pueda ser la menos idónea para propiciar las alertas. No obstante, es impensable que las entidades públicas de amplio tamaño limiten las posibilidades al envío de una carta y que no cuenten también con buzones online. Sin

embargo, por improbable, no elimina una posibilidad que es más factible conforme se reduce la dimensión de las entidades públicas, se dispone de menos recursos, o existe una prisa manifiesta para improvisar el cumplimiento de la Ley de cualquier manera. En mi opinión, solo se podrá hablar de un cumplimiento acorde a la vocación que se espera de estos sistemas cuando se articule una variedad de modalidades, entre las que haya necesariamente un buzón online. Este planteamiento va en lógica consonancia con la apuesta por la comunicación electrónica que imponen nuestras normas de procedimiento administrativo; y con la práctica, cada vez más asentada, de facilitar una relación multicanal entre las administraciones públicas y la ciudadanía, incluso, explorando las nuevas posibilidades que nos ofrecen los sistemas basados en inteligencia artificial como propone Campos Acuña (2022 p. 223).

6.2. Condicionantes técnicos para cumplir con las características del sistema

De cualquier manera, habrá que tener en cuenta que la utilización de una u otra vía —por escrito o solo verbalmente—, afecta a las obligaciones que se imponen a los sujetos obligados. Así, las alertas verbales deberán documentarse mediante grabación o transcripción —posteriormente firmada por el alertador— (art. 7.2).

Con independencia de la opción elegida, como ya se ha dicho, los canales deberán estar diseñados de tal modo que permitan la comunicación de todos los posibles alertadores según lo dispuesto en el artículo 3.1 y 3.2. En otras palabras, tanto de personas en activo en la organización, como desde fuera por quienes hayan tenido algún tipo de relación, motivo por el que estos sistemas no deben conocer de barreras de acceso físicas o virtuales. Así, no cumplirían con este estándar los cauces a los que no se pueda acceder por personas que no estén en la organización, o los virtuales que requieran la entrada a una VPN o de la previa posesión de credenciales de acceso o permisos.

Del mismo modo, se debe permitir la formulación de alertas anónimas, lo que constituye un reto como pone de manifiesto Iglesias Rey (2022 p. 185), porque la generalidad de las entidades públicas solo tiene experiencia bajo la dinámica de los procedimientos administrativos que exigen la identificación previa del interesado. De hecho, las implicaciones técnicas son especialmente relevantes en la utilización de medios telemáticos, porque no se puede hablar de una absoluta certeza de anonimato en internet, pero sí se puede prevenir que, inconscientemente, se recojan datos que permitan la identificación del alertador, como puede suceder con el registro de las IP u otros mecanismos que capturan información de manera automática. Son aspectos que no solo atañen a los servicios de informática de los sujetos obligados, sino también a sus proveedores tecnológicos. En esta línea, Vestri (2019) incide en la importancia de utilizar sistemas que permitan encubrir los datos entrantes y salientes, sin perjuicio de que los alertadores que quieran extremar las precauciones, usen aplicaciones como los navegadores que disponen de estas funcionalidades (el ejemplo clásico sería el navegador Tor que no deja rastro de la IP).

Lo mismo podríamos decir sobre las grabaciones de voz que hacen reconocible a una persona, o con la gestión de la documentación recibida por correo postal, cuyo matasellos puede dar pistas sobre la persona informante. Son aspectos que deberán estar recogidos en los procedimientos del sistema de gestión de la información, o de los que, en su defecto, debería tomar buena nota la persona responsable del sistema para no vulnerar la garantía de confidencialidad y la vocación de anonimato.

Además, conviene reiterar que existen experiencias en las que estos canales telemáticos están integrados en una herramienta que, no solo permite la recepción de alertas, sino la comunicación bidireccional entre quienes gestionan el sistema y el alertador —algo necesario para facilitar el acuse de recibo, la respuesta al informante u otras comunicaciones (ex art. 9.2)—. Esta funcionalidad se puede habilitar respetando las condiciones de anonimato para lo que se emplean juegos de claves que se generan automáticamente y que no requieren la consignación de datos de identificación[30]. Con este tipo de sistemas que están presentes en buzones online como los que han puesto en marcha las oficinas y agencias antifraude de Cataluña, la Comunidad Valenciana o las Islas Baleares, se permite este tipo de comunicación y, con ello, decaen muchos de los argumentos que se han estado esgrimiendo durante el proceso de transposición y con anterioridad respeto a la inconveniencia de aceptar denuncias anónimas (véase Aliaga Rodríguez, 2022; y Sierra Rodríguez, 2020a).

6.3. Integración de canales y habilitación para recibir otras comunicaciones

Con todo, lo que sí parece estar claro, es que la redacción de la Ley está orientada a que queden vinculados al sistema de información canales diversos cuando exista más de uno, porque estén diferenciados por el tipo de infracciones al que se orientan o

porque se trate de canales que posibilitan comunicaciones a través de modalidades distintas.

El artículo 7.4 también permite que se utilicen para recibir comunicaciones que nada tengan que ver con la información que entra dentro del ámbito de aplicación de la Ley. Este precepto puede ir en la línea de facilitar que también sean los de uso cotidiano para la comunicación de otras irregularidades distintas, sujetas a otros regímenes o de menor entidad, así como las relativas a supuestos como podrían ser las quejas y sugerencias o las comunicaciones sobre el mal funcionamiento de los servicios públicos.

Los principales reparos que podemos poner a esta previsión, es que se terminen produciendo accesos no autorizados a las comunicaciones porque los canales, dada su versatilidad, puedan ser consultados o accesibles a personas ajenas a la gestión del sistema; o que estos canales se utilicen de modo desvirtuado para comunicaciones ordinarias muy alejadas de la detección de irregularidades, aumentando el riesgo de producir brechas de seguridad o quedar expuestos a ataques externos, como puede suceder con mayor probabilidad ante comunicaciones electrónicas.

7. Políticas del sistema y procedimientos de gestión de la información

Un segundo elemento de análisis son las políticas y el procedimiento de gestión de informaciones. De ambos, el más tratado en la Ley es el procedimiento de gestión sobre el que centraremos nuestra atención, ya que, sobre las políticas o estrategia del sistema, el artículo 5.2 *h)* se limita la indicar que consistirá en una compilación de los principios generales sobre el sistema interno de información y defensa de la persona informante que deberá ser publicitada en la organización.

Las previsiones de la Ley no son lo suficientemente detalladas como para que podamos inferir todo lo que debe tener el sistema de información interno y el procedimiento de gestión de información, más allá de su sucinta caracterización y de los rasgos resultantes que se esperan según la Ley. Sobre estos procedimientos y a la vista de lo establecido en la Directiva, García Moreno (2020 p. 253) ya incidía en que, dentro del marco normativo, serán las organizaciones las que tengan libertad para decidir sus aspectos concretos a través de una norma interna que deberá estar adaptada a sus valores, estructura y funcionamiento. Aun así, una vez que la Ley está publicada, tal y como se comprobará en las siguientes páginas, nos siguen faltando previsiones para conocer cómo deben articularse los sistemas internos y estos procedimientos internos.

7.1. Los contenidos del procedimiento de gestión de información

El artículo 9 regula el procedimiento de gestión de informaciones, del que se extrae que sus contenidos deben explicitar los pasos necesarios y el tipo de tratamiento que se dará a las comunicaciones recibidas por el sistema de información interno. Este procedimiento deberá ser aprobado por el órgano de administración o de gobierno de cada sujeto obligado, y tener un contenido mínimo cuya enumeración nos ayudan parcialmente a fijar su alcance en los aspectos básicos que deben cumplir las organizaciones a la hora de gestionar la información[31].

Así, figura como contenido mínimo la identificación de los canales internos asociados al sistema —art. 9.2 *a)*—, lo que implica, dar a conocer a través de soportes visibles qué canales lo integran, sobre todo, para permitir su distinción con otras vías de comunicación que pueda tener la organización. Esta identificación deberá dejar claro cuáles son los canales sobre los que se proyectan las garantías de seguridad y confidencialidad, que serán aquellos que dispongan de las características técnicas que no tienen por qué estar presentes en el resto de vías de comunicación. De hecho, la Ley no se olvida de la posibilidad de errar y de que se usen cauces distintos a los que formalmente están previstos, por lo que impone que el procedimiento debe recoger la garantía de la confidencialidad en estos supuestos, bien porque se remitan las alertas a través de canales no contemplados para ello, o porque se envíen a cualquier persona que no sea 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» —art. 9.2 *g)*—.

El procedimiento también debe incluir la disposición de información «clara y accesible» sobre los canales externos —art. 9.2 *b)*—, lo que viene a ser una traslación del doble papel que pueden ejercer estos cauces, tanto como vía alternativa a los de carácter interno, como de complemento en caso de que se observe que la información enviada no haya sido seguida de manera diligente.

En lo que respecta a las comunicaciones con la persona informante, el procedimiento debe recoger el envío de un acuse de recibo en un plazo de siete días naturales tras la recepción de la alerta —art. 9.2 *c)*— y fijar el plazo en el que se le deberá dar respuesta sobre las actuaciones de investigación, que no deberá ser superior a tres meses —art. 9.2 *d)*—[32]. También debe contemplar cuáles son las posibilidades para mantener comunicaciones con el informante o requerirle que aporte información adicional o aclare la ya aportada —art. 9.2 *e)*—. Este extremo es especialmente relevante cuando los indicios sobre infracciones guardan verosimilitud, pero siga faltando información crucial para la determinación de la calificación de los hechos o sobre la participación de las personas afectadas, entre otros posibles supuestos. Ello conlleva que los sistemas, pese a la confidencialidad, deben contener cauces o fórmulas seguras de comunicación con el alertador, sin perjuicio de algunas excepciones para no poner en riesgo la confidencialidad —art. 9.2 *c)*—. En todo caso, pudiera pensarse que este tipo de comunicaciones con el alertador no son posibles ante alertas anónimas, pero tal y como ya se ha dicho, las nuevas tecnologías facilitan que las personas informantes puedan formular una alerta sin ofrecer dato de identificación alguno, y obtener la asignación de unos códigos de acceso que le permitan acceder a un buzón virtual en el que comunicar o recibir información y notificaciones.

Con relación al plazo de respuesta a la persona informante, quien gestione el sistema deberá realizar las comprobaciones pertinentes en ese plazo máximo de tres meses. No obstante, Sáez Hidalgo (2021) remarca que no necesariamente se deben finalizar las actuaciones en ese periodo, sino que se trata de un plazo máximo para informar —«para dar respuesta a las actuaciones de investigación» dice el art. 9.2 *d)*—, a diferencia de lo establecido para el canal externo que indica expresamente que el plazo para finalizar las actuaciones será de tres meses (art. 20.3). De igual modo, más allá del plazo ordinario y ante casos complejos, el plazo para informar se puede ampliar un máximo de tres meses adicionales —art. 9.2 *d)*—. La Ley no recoge la obligación de motivar esta decisión por la que se aplique un mayor plazo o de comunicar a la persona informante, pero dado el énfasis de la Directiva sobre la comunicación con el informante, no sería desaconsejable recoger este extremo en el procedimiento a seguir.

También debe contener previsiones sobre los afectados, como es su derecho a ser informado sobre las acciones y omisiones que se le atribuyen —en el momento pertinente para no perjudicar la investigación—, así como a ser oído —art. 9.2 *e)*—. De hecho, se debe observar el respeto a la presunción de inocencia y al honor de las personas afectadas durante la aplicación del procedimiento —art. 9.2 *h)*—.

Se preceptúa, además, que entre los contenidos del procedimiento hay que incorporar las garantías sobre protección de datos —art. 9.2 *i)*— que se regulan en el Título VI (arts. 29-34). Es decir, que, además, de las obligaciones genéricas en materia de protección de datos, se deben concretar singularidades de extremada importancia para garantizar la confidencialidad. Por tanto, el procedimiento debería delimitar quienes tendrán acceso a la información sobre datos personales y en qué condiciones, pero añadiendo otras concreciones para cumplir con la exigencia de contar con medidas organizativas y técnicas adecuadas para la preservación de la identidad, tanto de la persona informante como de las afectadas. Entre ellas podríamos pensar en medidas de seguridad informática (limitación de accesos, encriptación de archivos, etc.), anonimización preventiva de los documentos que se utilicen durante el seguimiento de las alertas, entre otras muchas posibilidades. Cabe resaltar que, según el artículo 32, podrán tener acceso a los datos la persona responsable del sistema y quién lo gestione directamente, y a partir de ahí, se puede ir abriendo el abanico en función de diversos condicionantes a personas con responsabilidad en distintas áreas: de recursos humanos u órgano competente cuando procedan medidas disciplinarias; de los servicios jurídicos si es necesario adoptar medidas legales; entre otros (véase el art. 32).

Como se puede intuir, los contenidos mínimos del artículo 9 no son suficientes para asegurar el funcionamiento del sistema y los procedimientos se deberán pormenorizar aún más, particularmente, en lo que se refiere a las fases de investigación y a otros aspectos que se erigen como obligaciones en la Ley, como por ejemplo el registro obligatorio de informaciones del canal interno (ex art. 26); de la forma solicitar y llevar a cabo la comunicación de información a través de entrevista (art. 7.2); los medios de grabación y documentación de la información y su posterior custodia y trazabilidad (art. 7.2), entre otros. Para ello, será útil revisar la especificación de las características y el procedimiento que se prevé para los canales externos (Título III), que regula desde la recepción de la información (art. 17) —a cuya imitación podrían concretarse las características de los canales internos previstos en el artículo 7—, como todos los pasos ulteriores: el trámite de admisión (art. 18), la instrucción (art. 19) o la terminación de las actuaciones (art. 20), siendo relevante que los procedimientos recojan cuál es el destino de la información cuando se concluya que ha existido una infracción.

Por otra parte, aunque no lo exige la Ley, convendría que el procedimiento recoja qué se debe hacer con aquellas prácticas que hayan sido comprobadas y que no constituyan infracción, pero sí casos de mal funcionamiento de los servicios públicos o una actuación que no esté ajustada a los códigos éticos o a su consideración como una práctica administrativa diligente y profesional. Se puede articular su derivación o un procedimiento específico que, en principio, quedaría ajeno a muchas de las garantías de la Ley cuando estas comunicaciones no entren dentro de su ámbito material de aplicación.

En suma, tras lo examinado nos situamos en la línea de León Alapont (2022 p. 196) quien señalaba que viene a resultar incomprensible y juega en contra de la seguridad jurídica toda esta insuficiencia de la regulación del procedimiento de gestión en el ámbito interno. Entre tanto y mientras no llegue su reglamento o recomendaciones emanadas de las autoridades independientes, será de utilidad observar modelos y estándares sobre la materia como las normas UNE-ISO, y, específicamente la UNE-ISO 37002 sobre sistemas de gestión de denuncias de irregularidades para cuyo análisis se remite al texto de Gutiérrez Rodríguez (2022 p. 83 y ss.)[33].

7.2. Sobre el seguimiento de hechos constitutivos de delito y su remisión al Ministerio Fiscal

Entre los contenidos mínimos expuestos, faltaba mencionar que el art. 9.2 *j)* prevé la remisión inmediata de la información al Ministerio Fiscal cuando los hechos «pudieran ser indiciariamente constitutivos de delito», o a la Fiscalía Europea si afectan a los intereses financieros de la Unión —en los mismos términos se expresa el art. 18.2 *c)* para el canal externo—. Este precepto requiere su estudio con mayor detenimiento porque afecta sustantivamente a las posibilidades de gestión de la información recibida cuando estamos ante ilícitos penales.

Como afirmaba Parajó Calvo (2022 p. 52) la tramitación de la información en estos casos, queda limitada a su remisión al Ministerio Fiscal. Así es, porque el precitado artículo expresa que se remitirán «con carácter inmediato cuando los hechos pudieran ser indiciariamente constitutivos de delito». Centrándonos en los posibles delitos, se observa que la obligación de remisión rige «con carácter inmediato» y conlleva que no se pueda esperar a finalizar la investigación, pero podemos sostener que sí exige un mínimo de análisis preliminar. Si observamos el esquema dado al procedimiento del canal externo, vemos que el idéntico mandato de remisión al Ministerio Fiscal se ubica en la regulación del trámite de admisión —art. 18.2 *c)*—. Por tanto, entendemos que el momento de remisión equivalente en los procedimientos internos debería ser tras el análisis inicial de la verosimilitud del contenido de la información. Del mismo modo, es previsible que una información sobre la que inicialmente no se observe un posible delito, evolucione a raíz de las actuaciones y termine en su envío al Ministerio Fiscal, extremo que se deberá recoger en el correspondiente procedimiento de gestión de información, tal y como lo hace el artículo 20.2 *b)* para el canal externo. Con todo, lo que queremos evidenciar es que los sistemas de información interna tendrán la posibilidad de investigar infracciones del Derecho de la UE y de aquellas que sean graves o muy graves en el ámbito administrativo, pero su capacidad de actuación queda mutilada cuando estemos ante un delito o queden afectados los intereses financieros de la Unión.

Pese a su aparente simplicidad, el cumplimiento de este mandato requerirá de algún tipo de recomendación por parte de la autoridad independiente o de una circular de la Fiscalía, para que se ayude a los sujetos obligados a determinar el tipo de actos y modo de apreciación de los indicios constitutivos de delito. Entre las aclaraciones adicionales que se precisan, está la definición del tipo de delitos que originan la obligación de remisión, dado que la información recibida puede versar sobre delitos que no tengan la calificación como graves o muy graves, o que se trate de delitos semipúblicos o privados en los que no quepa la actuación de oficio de la Fiscalía. De lo contrario, y ante la duda, el recurso fácil ante la obligación impuesta y la posible exigencia de responsabilidad, será remitir esta información a la Fiscalía con el consecuente riesgo de saturación o falta de atención respecto a este tipo de comunicaciones.

Por ello, nos alineamos con Bueno Sánchez (2021 p. 224) quien incide en que en la esencia del derecho penal está su consideración como derecho de intervención mínima y advierte del riesgo de judicializar todas las conductas que «supongan irregularidades administrativas para, ya en el seno del proceso, determinar si dichas irregularidades han dado lugar por su gravedad a la comisión de un delito». Recuerda el autor que el proceso penal es más lento debido a su carácter garantista y que un exceso de casos desvirtuaría la lógica de este sistema y terminaría generando un colapso, que sería contradictorio a la finalidad de perseguir los que tengan una mayor sustancia penal. El autor hace sus reflexiones con relación a la autoridad independiente, de la que se presume que estará más especializada y realizará el correspondiente cribado, motivo

por el que esta observación cobra mayor sentido si la aplicamos a los sujetos obligados que dispondrán —seguramente— de menores recursos y especialización para discernir sobre qué y bajo qué criterios procede remitir la información al Ministerio Fiscal.

No obstante, otros autores como Gimeno Beviá (2022, p. 352 y 353) dejan entrever cierta desconfianza a cualquier margen de apreciación sobre la existencia de ilícitos penales en el marco de estos sistemas, al caracterizar a las autoridades como un filtro de denuncias «en detrimento de las autoridades judiciales, policiales y del Ministerio Fiscal». Se deduce que la posición del autor otorga un mayor peso a las garantías —también en términos de derecho de defensa— que ofrece el Ministerio Fiscal.

7.3. La trascendental inadmisión que no está perfilada en la Ley

Un aspecto que nos preocupa particularmente es lo que ocurra respecto a la admisión de las comunicaciones en el seno de los sistemas internos de información. La laguna sobre su regulación en los sistemas internos, ocasiona que no queden delimitados cuáles son los criterios a respetar, lo que puede dar lugar a un abuso de la inadmisión por contemplar causas que se aparten de las recogidas en la Ley para el canal externo o porque éstas sean interpretadas de manera extensiva.

Además, las consecuencias de la inadmisión son importantes porque el artículo 35.2 *a)* excluye del acceso a la protección cuando las comunicaciones «hayan sido inadmitidas por algún canal interno de información o por alguna de las causas previstas en el artículo 18.2.a) [artículo referido a las causas de inadmisión en el canal externo]». Entendemos que esta exclusión de las protecciones no debe impedir que, tras una inadmisión en un sistema interno, la comunicación sí dé lugar a la protección siempre que, posteriormente, sea admitida en el canal externo. De lo contrario, si bastase la sola inadmisión en el canal interno para excluir de la protección, una actuación deliberada para acallar las denuncias tendría un fiel aliado en este precepto.

En todo caso, y dada la indefinición sobre las causas de inadmisión en el sistema interno, su repertorio debería ser lo más restrictivo posible, lo que en el ámbito público se traduce en que, como mucho, se ciñan a las causas de inadmisión previstas para el procedimiento administrativo común —siempre que estén en sintonía con la Ley—; a las derivadas del acotamiento al ámbito material y personal de aplicación de la Ley; y a la replicación de aquellas que se prevén —en este caso expresamente— en la regulación del canal externo en el artículo 18.2 *a)*. Entre estas últimas encontramos que los hechos carezcan de toda verosimilitud o manifiestamente de fundamento, no contengan información nueva y significativa respecto a anteriores comunicaciones recibidas que justifiquen su seguimiento, o cuando existan indicios racionales de haberse obtenido mediante la comisión de un delito, entre otras. Con relación a las causas de inadmisión, también se debería prever un mecanismo de revisión interna a instancia de la persona informante, al igual que ante otros posibles desenlaces que provoque una alerta, aunque habrá que examinar la viabilidad de este tipo de procedimientos en el sector público ante la consideración de las personas informantes no como interesadas, sino como meras colaboradoras de la administración.[34]

7.4. Breve referencia a los procedimientos para la protección de las personas alertadoras

Dado que estamos haciendo alusión al procedimiento de gestión de la información, hay que remarcar que en sus contenidos mínimos no se incluyen las garantías de protección. Al tratarse de un elemento básico del sistema interno, estas garantías deberían ser explicitadas en algún lugar con sus elementos básicos como las condiciones y la forma de acceder a ellas y los protocolos que se deben activar ante represalias, ya sea a través de un documento de procedimiento o a partir de la aplicación de las políticas generales del sistema.

De cualquier manera, habrá que explicitar y adaptar a la organización las medidas de protección del Título VII. Estas quedan diferenciadas en la Ley a partir de la prohibición de represalias —incluida su amenaza y tentativa—, y con independencia de si se producen de manera directa o indirecta (art. 36.1 y 2), indicando un pormenorizado catálogo de posibles conductas a modo de ejemplo (art. 36.2); junto a medidas de apoyo como el asesoramiento e información, la asistencia efectiva frente a represalias, la asistencia jurídica en los procesos penales, o incluso, de manera extraordinaria el apoyo financiero y psicológico, entre otras (art. 37). Aparte, hay una serie de cláusulas en el artículo 38 que están destinadas a evitar la responsabilidad que se quisiera exigir a las personas informantes.

En este punto, hay que recordar que la prestación de las medidas de apoyo del Título VII corresponde a las autoridades independientes (ex art. 41), «sin perjuicio de las medidas de apoyo y asistencia es-

pecíficas que puedan articularse por las entidades del sector público y privado»; es decir, al margen de las que se establezcan internamente. Por tanto, podrán existir medidas de apoyo y garantías en las organizaciones, dado que, como menciona García Moreno (2020 p. 282 y 283), que haya protecciones previstas por la normativa «no significa que la organización pueda desentenderse de esta tarea» porque el éxito del sistema dependerá en gran medida de que la organización tome un papel activo, y además, porque la respuesta ante represalias en el ámbito interno posiblemente será más ágil y adaptada que aquella que puedan ofrecer las autoridades independientes.

Así, bajo esta idea de explicitar y procedimentar el acceso a protecciones, también se debería recoger el modo de poner en conocimiento de la persona responsable del sistema las represalias que se pudieran estar sufriendo y los mecanismos para su cesación y, en su caso, restitución de la situación precedente. Además, la comisión de represalias es una infracción muy grave a efectos del régimen sancionador de la Ley —art. 63.1 *b)*—, por lo que debería existir un mecanismo para activar su comunicación desde los sistemas internos a la autoridad independiente, de modo que pueda ejercer su potestad sancionadora, sin perjuicio de su concurrencia con la facultad disciplinaria que pueda existir internamente en cada organización (art. 61.1).

Con todo, será necesario aterrizar los mandatos genéricos que se imponen a los sistemas internos para que establezcan las garantías de protección de los informantes en el interior de las organizaciones, pero también, respecto a otros aspectos en los que falta una referencia expresa o mayor concreción: las políticas del sistema, los derechos y garantías de quienes emiten alertas a imitación de los que se establecen en el artículo 21 para el canal externo, o la formación que se deba impartir en la materia a todas las personas que forman parte de la organización, entre otros muchos.

8. La persona responsable del sistema

La última pieza que analizamos de este engranaje es la persona responsable del sistema interno de información. Está regulada en el artículo 8 y se caracteriza como una figura independiente y autónoma dentro de la organización, cuya misión es estimular el seguimiento de las alertas y garantizar que el funcionamiento del sistema se ajusta a los parámetros de la Ley. Se trata de una persona a quien se le pueden exigir responsabilidades por su funcionamiento. De hecho, el artículo 9.1 incluye expresamente que «el Responsable del Sistema responderá de su tramitación diligente [con relación al procedimiento de gestión de informaciones]».

Parece un acierto que en el texto de la Ley se insista en la identificación de una persona física para el desempeño de estas funciones, de modo que se evite la dispersión a la hora de exigir responsabilidades por la falta de un cumplimiento diligente de las obligaciones de la Ley. Incluso, aunque se permita que la persona responsable del sistema sea un órgano colegiado (ex art. 8.2), la Ley indica que «este deberá delegar en uno de sus miembros las facultades de gestión del Sistema Interno de información y de tramitación de expedientes de investigación». A partir de esta descripción inicial haremos algunas reflexiones y comentarios críticos sobre su independencia y autonomía, grado de responsabilidad y respecto a su perfil.

8.1. Sobre su necesaria independencia y autonomía en el ejercicio de sus funciones

La Ley enuncia en su artículo 8.4 que la persona responsable del sistema debe «desarrollar sus funciones de forma independiente y autónoma respecto del resto de órganos de la entidad u organismo». En abstracto estas previsiones de la Ley son meramente declarativas porque el mantenimiento efectivo de esa independencia y autonomía de la persona responsable terminará dependiendo, principalmente, de su actitud personal, al igual que de su capacidad y proactividad para llevar de manera diligente el funcionamiento del sistema interno.

Debemos recordar que este cargo será designado por el órgano de administración o de gobierno de cada entidad sin que se establezca un perfil concreto —salvo en el sector privado donde se apunta a un directivo ex art 8.5—. Así, los riesgos en el sector público son evidentes si desde los órganos de gobierno se quiere controlar la información y se busca la designación de comisarios políticos.

Nos podemos preguntar si estas previsiones solo conllevarán que se busque a alguien de confianza que siga informalmente al servicio de quienes lo han designado, o que actúe bajo una dinámica movida únicamente por un afán de minoración u ocultamiento de las infracciones y/o de sus consecuencias. Entre los

Núm. 24 zk./2023. Págs. 70-98 or.
ISSN: 2173-6405 e-ISSN: 2531-2103

peligros más evidentes está que la persona responsable del sistema maniobre para buscar sutilmente acuerdos de transacción y evitar que las alertas afecten reputacionalmente a la organización, que se sigan lógicas exclusivamente corporativistas, o que se haga un seguimiento diferenciado de la información en función de quién sea el señalado, todo ello sin perjuicio de la filtración de información interesada, que en el ámbito público tiene una especial relevancia cuando afecta a la esfera política.

De hecho, Ponce y Villoria (2020) ya se plantearon algunas posibles condiciones para actuar de barrera ante las injerencias políticas, y venían a proponer que quienes tramitasen las alertas fuesen funcionarios de carrera nombrados por un plazo definido en el tiempo[35]. Con el marco normativo actual, no se favorece que los responsables sean personas independientes si su designación no se constriñe a criterios técnicos y bajo procedimientos transparentes y de concurrencia competitiva. Por ello, se echa en falta que la norma hubiera condicionado este nombramiento al cumplimiento de requisitos respecto a su perfil y a un procedimiento, extremo que podrá ser paliado por las normas de carácter interno que cada entidad pública establezca.

También podría tener cabida una evaluación de idoneidad acorde a la vocación de estos sistemas como piezas integrantes de un marco de integridad, y que, además, tuviera en cuenta la capacidad del responsable para impulsar la actividad del sistema interno ante el riesgo que supone la inacción ante infracciones que se hayan comunicado o represalias que se estén produciendo. De hecho, con cierta actitud escéptica respecto a los sistemas internos, Garrido Juncal (2022 p. 177) se expresaba en este sentido «la novedosa exigencia de que las denuncias se tramiten con diligencia o en un plazo razonable no vale de nada, si detrás no hay una intención firme de acatarla. No se puede ignorar aquí que la inactividad formal es una realidad cotidiana, a pesar de que los textos legales, que imponen la obligación de resolver en un tiempo concreto, se cuentan por decenas».

Por lo demás, las previsiones que se establecen en la Ley para asegurar esta autonomía e independencia son prácticamente nulas y se limitan a enunciar que no podrá recibir instrucciones en el ejercicio de su función y que deberá disponer de medios materiales y personales suficientes (art. 8.4); o a imponer la obligación de comunicar el nombramiento y cese del responsable del sistema[36], justificando en este último caso los motivos que hayan ocasionado su destitución (art. 8.3). Son garantías insuficientes que nos llevan a interrogarnos sobre el grado de generosidad en la dotación de medios para el sistema de información interna ante la presencia de casos y responsables del sistema que sean incómodos; o hasta qué punto se exigirá una justificación pormenorizada y se podrán revertir las decisiones sobre su cese cuando se deba a motivaciones espurias.

Con independencia de los riesgos a los que se ha hecho alusión, y pese al énfasis de la Directiva sobre los parabienes de los sistemas internos, no puedo dejar de manifestar mi desconfianza, como ya he hecho en ocasiones anteriores (Sierra Rodríguez, 2020b p. 69), sobre lo que ocurra en organizaciones de tamaño reducido en las que existe un cúmulo de relaciones duraderas que pueden condicionar —directa o indirectamente— la actuación de quienes están al frente de los sistemas internos, pero también la actitud que los potenciales alertadores tengan hacia el sistema. Como ya se ha encargado de remarcar Campos Acuña (2022 p. 219 y 220), este tipo de reflexiones adquieren una mayor virtualidad en ámbitos como la administración local por la proximidad que los define.

Por ello, la figura del responsable será aún más relevante y será determinante para el éxito del sistema que los potenciales alertadores «consideren a su interlocutor una persona con un elevado compromiso de integridad y confiable respecto a la ocultación de su identidad y al tratamiento de los hechos comunicados» (García Moreno, 2020 p. 273).

8.2. **La responsabilidad de la «persona responsable»**

En este contexto reiteramos que el papel de la persona responsable es una pieza clave del sistema, por lo que sería necesario que la futura autoridad independiente no dude en imponer sanciones ejemplarizantes cuanto éstos sean artífices de la falta de seguimiento de las alertas o por entrar en las dinámicas antes descritas. Al respecto, encontramos supuestos de infracción muy grave como el previsto en el artículo 63.1 *a)* ante «Cualquier actuación que suponga una efectiva limitación de los derechos y garantías previstos en esta Ley introducida a través de contratos o acuerdos a nivel individual o colectivo y en general cualquier intento o acción efectiva de obstaculizar la presentación de comunicaciones o de impedir, frustrar o ralentizar su seguimiento».

Hay previsiones que se proyectan específicamente sobre el sistema de información interna y así, el artículo 63.1 *g)* considera como infracción muy grave el «incumplimiento de la obligación de disponer de un sistema interno de información en los términos exigidos en esta ley». Otros supuestos de infracción y

sanción se proyectan sobre el cumplimiento defectuoso de las características básicas del sistema por vulneración de la confidencialidad y el anonimato, por transgredir el deber de mantener secreto, o por no adoptar las medidas para ello —infracción muy grave art. 63.1 *c)* y *d)* y grave art. 63.2 *b) c)* y *d)*—. A todo ello se añaden otras responsabilidades que recaigan en la persona responsable del sistema o en su equipo por aplicación de otras parcelas del ordenamiento jurídico, que pueden ver intensificada su severidad cuando estamos hablando de empleados públicos[37].

8.3. **Perfil de conocimientos**

Finalmente, hacemos una breve alusión al perfil del responsable porque viene escasamente caracterizado en la Ley. En el sector público debería ser una persona que, junto a su equipo, disponga de vastos conocimientos jurídicos y de recursos humanos que abarquen el derecho laboral, la gestión de personas y la prevención de riesgos laborales; el derecho administrativo —con singular énfasis en los distintos regímenes aplicables al empleo público—; con conocimiento de derecho penal; y, según el tipo y funciones de entidad pública, del régimen que sea de aplicación sectorial según la especialización o el carácter de la organización. A estos conocimientos, se unen las capacidades y habilidades que debe tener para montar o adaptar el sistema, seguir mínimamente las alertas, contribuir a la aplicación de las medidas de protección y dar salida a la información en caso de concluir que se han detectado infracciones.

La Ley prevé que se pueda nombrar a quien ya estuviese desempeñando funciones en torno a las políticas de integridad o asimiladas (art. 8.6) —no lo impone—. De cualquier manera, se trata de perfiles que no abundan y que costará formar, dado que, como ya se ha dicho, la experiencia sobre estos sistemas es escasa o nula porque, hasta la fecha, la denuncia administrativa caracterizada por la identificación previa, dista del nuevo concepto de alerta que se predica en la Ley (Miranzo Díaz, 2022).

9. Reflexiones finales

En este análisis de la regulación de la Ley 2/2023, se han tratado algunos aspectos capitales del nuevo sistema de alertas y protección que suscitan muchas incógnitas. Sobre ellos está fijando su atención la comunidad académica y profesional, porque se espera que haya un paulatino desarrollo que supere el que en su momento conllevó la legislación sobre transparencia pública. En este caso, las implicaciones que se derivan de las alertas son de un amplio calado y sus obligaciones son de mayor envergadura porque abarcan de manera generalizada a todas las entidades del sector público y a una parte importante del sector privado.

En este artículo, hemos reflexionado sobre las limitaciones del ámbito material de la Ley que, pese a todo, es amplio gracias al entrecruzamiento de su aplicación a las infracciones derivadas del Derecho de la Unión y las que, fuera de él, constituyen infracciones graves o muy graves de carácter administrativo o penal.

Sobre el ámbito de aplicación personal, se ha subrayado que ceñirlo al contexto laboral y profesional tiene su sentido con relación a la protección ante represalias, porque se trata de espacios en los que hay una mayor exposición a relaciones de dependencia o sujeción a terceros. Sin embargo, se podría haber abierto más, a personas ajenas a este tipo de nexo, haciendo posible la colaboración ciudadana en la detección de infracciones. No obstante, la existencia de una puerta de atrás en los sistemas de información interna, como se deduce de su regulación y de la combinación del anonimato con la exigencia de accesibilidad desde fuera, seguramente permitirá la formulación de alertas por terceros ajenos a las organizaciones, aunque no gocen de la calificación como informante y de la posibilidad de acceder a las medidas de protección.

Debemos enfatizar en la importancia de tener claro el carácter sistémico de todo este engranaje, como conjunto de piezas entrelazadas que deben estar perfectamente coordinadas en el seno de los sistemas de información. Ya no se trata de habilitar un buzón de denuncias, sino que deben extremarse las precauciones y disponer de medidas técnicas y organizativas que permitan las comunicaciones mediante diversas modalidades; de diseñar y seguir protocolos y procedimientos para su gestión en condiciones de seguridad y confidencialidad; de garantizar la protección ante represalias; o de contar con un responsable en las propias palabras del término, que junto a su equipo de trabajo, será susceptible de incurrir en responsabilidades y ser sancionados por la autoridad correspondiente ante un cumplimiento defectuoso de lo previsto en la Ley.

Con todas estas previsiones de la Ley y muchas otras que no se han podido abordar en este texto por cues-

tiones de espacio, lo que está claro es que, aun con insuficiencias, la norma tendrá un impacto considerable y ocupará una parcela propia como ha sucedido con otros ámbitos recientes que han sido impulsados por la vía normativa. Por ello, esta materia seguramente acaparará una amplia atención durante los próximos años y mientras dure todo el proceso de puesta a punto de los sistemas de información interna, del establecimiento de la Autoridad Independiente de Protección del Informante y del despliegue autonómico de lo previsto en la Ley.

El corto plazo de tiempo que se ha dado para tener en funcionamiento los sistemas de información interna, puede provocar que durante un primer estadio de su implementación se produzca un incumplimiento generalizado de las obligaciones de la Ley, o lo que es peor, un cumplimiento defectuoso y visible que dé lugar a un efecto de desconfianza sobre la formulación de alertas y lastre su utilización para los próximos años.

Solamente el transcurso del tiempo nos permitirá conocer realmente cómo se va desarrollando todo el sistema, pero lo que sí está claro es que hacen falta pautas de interpretación de la Ley. Son necesarias recomendaciones sobre el estándar a cumplir, que delimiten claramente las zonas grises de la regulación y que concreten mucho más los aspectos técnicos y los pormenores para la puesta en marcha de estos sistemas, porque es precisamente en ellos, en los que residen las posibilidades de su éxito o fracaso temprano.

En este camino será necesario disponer de un reglamento de la Ley, algo que tardará, y en su defecto, que estén funcionando las autoridades de protección. Sus circulares, las recomendaciones y la información que emitan se erigirán en una clave importante a tener en cuenta para actuar como guía, particularmente, para los sujetos obligados que no disponen de recursos humanos especializados en la materia y que conforman una constelación numerosa de organizaciones del sector público.

Pero no es la única razón, dado que un sistema como este quedará en papel mojado si no existe una instancia que vele por el cumplimiento de lo prescrito por la Ley y sancione de manera ejemplarizante las represalias y a quienes estando obligados, no cumplan con lo establecido para los sistemas de información interna, motivo por el que es imprescindible, no solo la creación de las autoridades estatal y autonómicas, sino que éstas sean realmente independientes, eficaces y que impongan un alto estándar respecto al cumplimiento de la Ley desde el primer momento.

Referencias bibliográficas

Aliaga Rodríguez, R. (2022). La denuncia anónima como instrumento de transparencia y protección de denunciantes. *Revista Española de la Transparencia*, 14, 57-78.

Bachmaier Winter, L. (2019). Whistleblowing europeo y compliance: La Directiva UE de 2019 relativa a la protección de personas que reporten infracciones de Derecho de la Unión. *Diario La Ley*, 9539, Sección Tribuna, 18 de diciembre de 2019.

Benítez Palma, E. (2018). El control externo y el *whistleblowing* (canales de denuncia). *Revista Española de Control Externo*, 59, 11- 42.

Boto Álvarez, A. (2022). Whistleblowing como contrapoder, también en el sector público francés. *Revista General de Derecho Administrativo*, 6, 1-10.

Bueno Sánchez, J. M. (2021). Oportunidad legal y necesidad democrática de crear una autoridad administrativa independiente de lucha contra la corrupción y protección del denunciante. *Revista de Administración Pública*, 217, 209-240.

Campos Acuña, C. (2022). Canales de denuncia y protección del denunciante en el ámbito local: Algunas dificultades propias de la administración local y propuestas de solución. En Gimeno Beviá, J. y López Donaire, M. B. (dirs), *La directiva de protección de los denunciantes y su aplicación práctica al sector público* (pp. 207-232). Tirant Lo Blanch.

Cerrillo i Martínez, A. (2018). Diez propuestas para la colaboración ciudadana en la alerta de malas prácticas en la Administración Pública. *Revista Internacional de Transparencia*, 6, 1-7.

Díez Garrido, M. y Campos Domínguez, E. (2020). ¿Actitud o imagen? La organización y percepción de la transparencia de los partidos políticos. *Estudios sobre el mensaje periodístico*, 26(4), 1411-1420.

Fernández López, M. (2018). Eficacia procesal de las declaraciones obtenidas en procedimientos de colaboración. *Derecho&Sociedad*, 50, 262-276.

Fernández Ramos, S. (2023). El ámbito material de aplicación de la Ley 2/2023 de Protección de los Informantes 1/2. *Hayderecho.com* (artículo fechado el 29 de marzo de 2023). https://www.hayderecho.com/2023/03/29/proteccion-a-los-informantes-ley-parlamento-europeo-lucha-contra-la-corrupcion/

García Moreno, B. (2020). *Del whistleblower al alertador. La regulación europea de los canales de denuncia*. Tirant Lo Blanch.

Garrido Juncal, A. (2022). La ley que protege a los informantes de infracciones normativas comienza su tramitación: preguntas y respuestas sobre una norma

indispensable para el buen funcionamiento de las instituciones democráticas. *Cuadernos Manuel Giménez Abad*, 24, 167-188.

Gimeno Beviá, J. (2022). Protección del denunciante y garantías procesales. En Gimeno Beviá, J. y López Donaire, M. B. (dirs), *La directiva de protección de los denunciantes y su aplicación práctica al sector público* (pp. 337-354). Tirant Lo Blanch.

Gimeno Beviá, J. y López Donaire, M. B. (dirs) (2022). *La directiva de protección de los denunciantes y su aplicación práctica al sector público*. Tirant Lo Blanch.

González Granda, P. (2021). La figura del alertador en la regulación proyectada en el Anteproyecto de la LECRIM y su trazabilidad constitucional. En González Granda, P. y Ariza Colmenarejo, M. J., *Justicia y proceso. Una revisión procesal contemporánea bajo el prisma constitucional* (pp. 367-385). Dykinson

Gutiérrez Rodríguez, M. (2022). Las normas UNE-ISO y su referencia a los canales de denuncia. En Gimeno Beviá, J. y López Donaire, M. B. (dirs), *La directiva de protección de los denunciantes y su aplicación práctica al sector público* (pp.71-100). Tirant Lo Blanch.

Iglesias Rey, P. (2022). El desafío del sector público ante la aplicación de la Directiva de protección del informante. Los canales de denuncia. *Revista Galega de Administración Pública*, *EGAP*, 64, 175-190.

Jiménez Franco, E. (2022). Prospectiva administrativa y la futura Ley de protección de los informantes. En Sánchez, Z. (Dir.), *Regulación con prospectiva de futuro y de consenso. Gobernanza anticipatoria y prospectiva administrativa* (pp. 215-242). Thomson Reuters Aranzadi.

León Alapont, J. (2022). Los canales de denuncia y la protección del informante en las entidades del sector privado: a propósito de la transposición de la Directiva (UE) 2019/1937, de 23 de octubre. *Revista de Derecho Penal y Criminología*, 28, 155-216.

Lozano Cutanda, B. (2020). La directiva de protección del denunciante. *Diario La Ley*, 9550, de 10 de enero de 2020.

Miranzo Díaz, J. (2019). La nueva Directiva europea de protección del denunciante: un análisis desde el Derecho Público. *Revista General de Derecho Europeo,* 49, 361-385.

Miranzo Díaz, J. (2022). El proyecto de Ley de protección del denunciante y su incidencia en la contratación pública. *Boletín del Observatorio de Contratación Pública*, 10-11 (octubre-noviembre).

Parajó Calvo, M. (2022). Análisis del proyecto de ley reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción. *Documentación Administrativa*, 9, 43-74.

Pérez Monguió, J. M. (2019). Del chivato al cooperador: el whistleblowing. *Revista Vasca de Administración Pública*, 115, 343-375.

Pérez Monguió, J. M. (2020). Whistleblower y las dificultades para su implementación en España e Italia. En Sánchez de Diego, M. y Sierra Rodríguez, J. (coords.), *Participación y transparencia para un gobierno abierto* (pp.225-245). Wolters Kluwer.

Pérez Triviño, J. L. (2018). Whistleblowing. *Eunomía. Revista en Cultura de la Legalidad*, 14, 285-298.

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*, 101-129.

Ponce Solé, J. y Villoria Mendieta, M. (2020). Estudio introductorio a la edición de 2020. *Anuario del Buen Gobierno y de la Calidad de la Regulación*, 31-75.

Ponce Solé, J. (2021). Regulación de las denuncias y derecho a una buena administración: reflexiones sobre discrecionalidad administrativa y whistleblowing. En Santana Vega, D. *et al.*, *Una perspectiva global del Derecho Penal. Libro homenaje al profesor Dr. Joan J. Queralt Jiménez* (pp.903-914). Atelier.

Puñal García, L. (2018). Whistleblowing y Transparencia en el Sector Privado de Alemania. *Dilemata*, 27, 203-219.

Rodríguez-Piñero, M. (2022) La protección de los trabajadores que informen sobre infracciones normativas. En Sánchez Bravo, A. (coord.), *Laborum et Scienciae. Libro Homenaje al Profesor Dr. Juan Raso Delgue* (pp. 17-38). Alma Mater.

Sáez Hidalgo, I. (2021). Los canales internos de denuncia en el sector público. *Actualidad Administrativa*, 7, Sección Actualidad, Julio-Agosto. Wolters Kluwer (LA LEY *7863/2021*).

Sierra Rodríguez, J. (2020a). Anonimato y apertura de los canales de denuncia de la corrupción. *Revista General de Derecho Administrativo*, 55.

Sierra Rodríguez, J. (2020b). Impulso europeo al whistleblowing y las autoridades de integridad. *Eunomía. Revista en Cultura de la Legalidad*, 19, 64-89.

Tardío Pato, J. A. (2022). La protección del denunciante para la garantía del cumplimiento de la legalidad y evitar la corrupción. *Revista Española de Derecho Administrativo*, 217, 11-60.

Vestri, G. (2019). Aproximación al sistema de whistleblowing. Un nuevo desafío para la administración pública española. *Revista General de Derecho Administrativo*, 51, 1-24.

Villoria Mendieta, M. (2021a). Un análisis e la Directiva (UE) 2019/1937 desde la ética pública y los retos de la implementación. *Revista Española de la Transparencia*, 21, 15-24.

Villoria Mendieta, M. (2021b). La protección al whistleblower: retos para la implementación en España. *Barataria. Revista Castellano-Manchega de Ciencias Sociales*, 31, 20-39.

Notas

1 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*, fijaba como plazo para su transposición hasta el 17 de diciembre de 2021. Sin embargo, el camino hacia la adopción de la norma llevaría otros ritmos más pausados. En fase prelegislativa se realizó la consulta pública en enero de 2021 y la audiencia e información pública un año más tarde en marzo de 2022. El proyecto de ley sería aprobado por el Consejo de Ministros para su remisión al Congreso en septiembre de 2022. A partir de ahí se seguiría el procedimiento de urgencia en sede parlamentaria completando su ciclo de tramitación y su aprobación el 16 de febrero de 2023.

2 Si hacemos referencia solo a los municipios hay 8.131 en España, mientras que en el Directorio Central de Empresas (DIRCE) del INE, en 2022 arroja la cifra de 24.714 empresas con 50 o más trabajadores. A estas dos cifras habrá que sumar las múltiples formas jurídicas distintas del sector público y privado que son sujetos obligados a tenor de lo establecido en la Ley.

3 Se ha reiterado profusamente la problemática que rodea al término denunciante y la inconveniencia de utilizar este término para el sistema que ahora se pone en marcha. De hecho, en su momento se criticó su utilización en la traducción de la Directiva al castellano (Jiménez Franco, 2022 p. 222-224) porque no respondía al nuevo concepto que se pretendía establecer, por las connotaciones sociales que arrastra (ej. chivato) y por su asociación a los cauces tradicionales de denuncia (administrativa y penal) que han venido siguiendo otra lógica. El sistema que ahora se dibuja se asocia a la expresión anglosajona «whistleblower» (quien toca el silbato), con relación a una persona que «creyendo que el interés público prevalece sobre el interés de la organización para la que trabajan, toca el silbato para anunciar que la organización está llevando a cabo una actividad corrupta, ilegal, fraudulenta o perjudicial» (Puñal García, 2018 p. 205). Se trata de una expresión que arroja amplias dificultades de traducción, motivo por el que se abogaría por otras como alertador o informante, siendo esta última la utilizada en la Ley. Sobre la cuestión terminológica y las diferentes perspectivas bajo las que se concibe al alertador se puede consultar el texto de Pérez Triviño (2018); y, singularmente, las referencias reflejadas por Pérez Monguió (2019 p. 352) sobre las dificultades de traducción del término whistleblower al contexto cultural italiano.

4 Es cierto que no todas las posibilidades de denuncia en el sector público estatal han venido guardando estas características tan poco motivadoras para los alertadores. Por ejemplo, contamos con precedentes que han permitido la comunicación de infracciones tributarias (art. 114 Ley 58/2003, de 17 de diciembre, General Tributaria) y que se han articulado a través de la web de la AEAT sin necesidad de dar los datos del denunciante. Se han generado buzones que permiten no consignar datos de identificación como el de la Comisión Nacional de los Mercados y la Competencia, o el de la Comisión Nacional del Mercado de Valores. A estos ejemplos, hay que sumar que, en ámbitos concretos, ya existía la obligación de contar con canales de denuncia asimilados a los sistemas que ahora se imponen, como así exigía la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo. En todo caso, pese a su existencia, no han sido la pauta generalizada en España. Sobre estas y otras experiencias previas como el buzón de denuncias del Ministerio de Trabajo, véase el texto de Benítez Palma (2018 p. 26-28).

5 Con anterioridad a la publicación de la Directiva, varias comunidades autónomas —también administraciones locales— han llevado la delantera en esta materia, aunque algunas de ellas solo regulasen los cauces de denuncia de los empleados públicos o se centrasen en la disposición de lo que actualmente quedan configurados como canales externos. Así, entre las comunidades autónomas, podemos citar aquellas que aprobaron leyes con anterioridad a la Directiva y que identificamos como una regulación parcial de sus contenidos: Ley 14/2008, de 5 de noviembre, de la Oficina Antifraude de Cataluña; Ley 2/2016, de 11 de noviembre, por la que se regulan las actuaciones para dar curso a las informaciones que reciba la Administración Autonómica sobre hechos relacionados con delitos contra la Administración Pública y se establecen las garantías de los informantes de Castilla y León; Ley 11/2016, de 28 de noviembre, de la Agencia de Prevención y Lucha contra el Fraude y la Corrupción de la Comunidad Valenciana; Ley 16/2016, de 9 de diciembre, de creación de la Oficina de Prevención y Lucha contra la Corrupción de las Islas Baleares; Ley 5/2017, de 1 de junio, de Integridad y Ética Públicas de Aragón; Ley Foral 7/2018, de 17 de mayo, de creación de la Oficina de Buenas Prácticas y Anticorrupción de Navarra; o la Ley 8/2018, de 14 de septiembre, de Transparencia, Buen Gobierno y Grupos de Interés de Asturias. Con posterioridad y sin ánimo de exhaustividad se han aprobado otras normas como la Ley 2/2021, de 18 de junio, de lucha contra el fraude y la corrupción en Andalucía y protección de la persona denunciante; o el Decreto 63/2022, de 20 de julio, del Consejo de Gobierno, por el que se establece y regula el canal interno para el tratamiento de las informaciones sobre posibles infracciones en la Comunidad de Madrid.

6 Una nítida justificación de esta apuesta por el sistema de protección la podemos encontrar en el considerando uno de Directiva que se expresaba en los siguientes términos: «las personas que trabajan para una organización pública o privada ... son a menudo las primeras en tener conocimiento de amenazas o perjuicios para el interés público que surgen en ese contexto ... Sin embargo, los denunciantes potenciales suelen renunciar a informar sobre sus preocupaciones o sospechas por temor a represalias».

Núm. 24 zk./2023. Págs. 70-98 or.
ISSN: 2173-6405 e-ISSN: 2531-2103

7 Rodríguez-Piñero (2022 p. 27) hace un paralelismo sobre esta lógica de protección con la garantía de indemnidad frente a las represalias empresariales, pero con la diferencia de que en la garantía de indemnidad, la situación habitual deriva de las acciones de reclamación ante incumplimientos de la normativa laboral que afectan personalmente al trabajador, mientras que, en este caso, «se propone la protección del denunciante que defienda —objetivamente— el respeto de ese Derecho, sean cual sean los motivos personales para hacerlo, y dadas el tipo de infracciones que incluye, en general las denuncias, no se realizarán para un personal o directo beneficio, posibilidad que, sin embargo, la propia Directiva no excluye».

8 La estructura de la Ley se resume como sigue. El Título I (arts. 1-3) comienza con la expresión de la finalidad de la ley y su ámbito de aplicación. El Título II (arts. 4-15) contiene las disposiciones generales para los sistemas internos de información y la especificación diferenciada de prescripciones para los sectores público y privado. El canal externo de información es regulado en su Título III (arts. 16-24), las obligaciones de publicidad y registro en el Título IV (arts. 25 y 26), la revelación pública en el Título V (arts. 27-28) y la protección de datos personales en el Título VI (arts. 29-34). A las medidas de protección ante represalias se dedican los artículos 35 a 41 (Título VII), mientras que la Autoridad Independiente de Protección del Informante es regulada en el Título VIII (arts. 42-59) y el régimen sancionador en el Título IX (arts. 60-68).

9 En concreto, se modifica la Ley 1/1996, de 10 de enero, de asistencia jurídica gratuita; la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa; la Ley 15/2007, de 3 de julio, de Defensa de la Competencia; la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo; la Ley 10/2014, de 26 de junio, de ordenación, supervisión y solvencia de entidades de crédito; la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público; y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

10 Los ámbitos enumerados en el artículo 2.1 *a)* de la Directiva son los siguientes: «i) contratación pública, ii) servicios, productos y mercados financieros, y prevención del blanqueo de capitales y la financiación del terrorismo, iii) seguridad de los productos y conformidad, iv) seguridad del transporte, v) protección del medio ambiente, vi) protección frente a las radiaciones y seguridad nuclear, vii) seguridad de los alimentos y los piensos, sanidad animal y bienestar de los animales, viii) salud pública, ix) protección de los consumidores, x) protección de la privacidad y de los datos personales, y seguridad de las redes y los sistemas de información».

11 Éstas se contemplan en las letras *b)* y *c)* del artículo 2.1 de la Directiva y se reproducen en la Ley nacional: «b) infracciones que afecten a los intereses financieros de la Unión tal como se contemplan en el artículo 325 del TFUE y tal como se concretan en las correspondientes medidas de la Unión; c) infracciones relativas al mercado interior, tal como se contemplan en el artículo 26, apartado 2, del TFUE, incluidas las infracciones de las normas de la Unión en materia de competencia y ayudas otorgadas por los Estados, así como las infracciones relativas al mercado interior en relación con los actos que infrinjan las normas del impuesto sobre sociedades o a prácticas cuya finalidad sea obtener una ventaja fiscal que desvirtúe el objeto o la finalidad de la legislación aplicable del impuesto sobre sociedades».

12 A su vez, esto ocasiona dos problemas adicionales que el autor pone sobre la mesa. El primero consiste en que hay ámbitos en los que solo constan parte de todos los actos normativos que existen, es decir, que se ha optado por incluir dentro de la aplicación de la Directiva solo algunas parcelas de cada uno de los ámbitos enumerados. El segundo, es que la relación de actos normativos que se citan en el Anexo constituye una referencia dinámica, de modo que, si son sustituidos o modificados por otros actos, los últimos deberán ser que se consideren como parámetro para delimitar el ámbito de aplicación de la Directiva. Para mayor complejidad, Fernández Ramos, subraya que los actos de la Unión pueden modular su propio ámbito de aplicación y que existen medidas delegadas y de ejecución nacionales derivadas de los actos de la UE —como sucede con la transposición de Directivas— que se deberán tener en cuenta a la hora de determinar qué infracciones entran dentro del ámbito de aplicación.

13 Hay que recordar que el artículo 32 establece algunas limitaciones a la conservación de las comunicaciones. En su apartado 3 indica «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 (...)», mientras que en su apartado 4 expresa: «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».

14 A partir del XI Encuentro de la Red de Oficinas y Agencias Antifraude celebrado en Cartagena en septiembre de 2022, algunas de ellas de ámbito autonómico consensuaron un documento de propuesta de enmiendas al proyecto de Ley. Así, indicaban que el ámbito material de aplicación debía ser más extenso, citando el considerando 42 de la Directiva, en el que se establece que «La detección y la prevención efectivas de perjuicios graves para el interés público exige que el concepto de infracción incluya también prácticas abusivas, (...) a saber, actos u omisiones que no parecen ilícitos desde el punto de vista formal, pero que desvirtúan el objeto o la finalidad de la ley» (Véase el documento de propuestas hecho público el 18 de octubre de 2022 en: https://antifrau.cat/sites/default/files/2022-10/proposta-esmenes-projecte-llei-reguladora-proteccio-persones-infor-

Núm. 24 zk./2023. Págs. 70-98 or.
ISSN: 2173-6405 e-ISSN: 2531-2103

min-sobre-infraccions-normatives-lluita-contra-corrupcio.pdf). Por otra parte, hay que dejar constancia que hubo algunas enmiendas parlamentarias que iban en esta línea, entre ellas, la número 94 del Grupo Parlamentario Republicano (BOCG Congreso de los Diputados, Serie A, núm. 123-3/2022, de 28 de noviembre [https://www.congreso.es/public_oficiales/L14/CONG/BOCG/A/BOCG-14-A-123-3.PDF]).

15 Conviene distinguir estos dos supuestos, que conllevan la diferenciación entre la producción de un delito solamente por el hecho de revelar la información, y el que se produce por la forma en la que se obtiene o accede a la información. Al respecto y sobre el primer supuesto, León Alapont (2022 p. 188) plantea que, en determinados casos, se podría alegar la existencia de circunstancias eximentes con base en el cumplimiento de algún deber o ejercicio legítimo de un derecho (ex art. 20.7.º CP) o por estado de necesidad para evitar un mal propio o ajeno (ex. art. 20.5.º CP).

16 De hecho, organizaciones de activistas como XNET recordaban que con las previsiones que se contemplaban en el proyecto de ley —ahora en la Ley—, tanto por el tipo de infracciones como por la no afectación a las responsabilidades de carácter penal, casos como el de Snowden o Falciani no se verían amparados. Sobre la postura de XNET, véase el texto «Urgente: enmiendas al proyecto de ley de protección de informantes/alertadores/whistleblowers»: https://xnet-x.net/es/xnet-enmendar-anteproyecto-ley-proteccion-informantes-ministerio-justicia/ (10 de enero de 2023).

17 En el ámbito público hay colectivos, como los funcionarios, que tienen una menor vulnerabilidad en comparación a otras figuras y, aunque sea difícil pensar en el equivalente a un despido, es igualmente importante el acento que se pone sobre la definición de las represalias como algo desfavorable, porque, igualmente, pueden verse afectados por acciones de regreso que se proyecten sobre la promoción interna, la concesión de destinos, o la asignación de tareas menos atractivas (García Moreno, 2021 p. 306).

18 En el mismo sentido se expresa Jiménez Franco (2022 p. 228) recogiendo otros ejemplos como el formulado por la Secretaria General de Hay Derecho, Safira Cantos, sobre los militantes de los partidos políticos con relación a casos de corrupción en su respectiva formación política.

19 Esta es una consecuencia derivada de la conceptualización restrictiva de lo que se entiende por «facilitador» con acceso a protección. La Directiva los configuraba como una persona física que ayuda al alertador en el marco de la organización en la que se trabaja, por lo que esta definición no abarca a quienes les asistan desde fuera o si se trata de personas jurídicas. A esta definición se ha circunscrito la ley española, mientras que, en Francia, como se ha encargado de señalar Boto Álvarez (2022 p. 8) se ha optado por una ampliación del entorno privado de apoyo, definiendo a los *facilitateurs* «como cualquier persona física o persona jurídica de derecho privado sin ánimo de lucro, que ayude a un denunciante a efectuar una denuncia o divulgación de conformidad con la Ley».

20 De hecho, se observan algunas omisiones respecto a intermediarios cuya participación es imprescindible en algunas vías para informar sobre infracciones. La Directiva expresa su considerando 45 que la protección de represalias debería abarcar a quienes ponen la información a disposición de la ciudadanía a través de la revelación publica, citando expresamente cauces como las «plataformas web o de redes sociales, o a medios de comunicación, cargos electos, organizaciones de la sociedad civil, sindicatos u organizaciones profesionales y empresariales». Sin embargo, en el articulado de la Ley no encontramos referencias sobre estos colectivos, o estipulaciones que permitan ofrecerles protección. No obstante, cabe decir que estas omisiones se pueden paliar parcialmente a través de normas complementarias, como estaba en proceso mediante el proyecto de Ley Orgánica de protección del secreto profesional del periodismo —en tramitación parlamentaria hasta la disolución anticipada de las Cortes Generales—, que derivaba de una enmienda *in voce* de la ponencia que examinó la Ley 2/2023 (véase BOCG Congreso de los Diputados, Serie A, núm. 135-1/2022, de 19 de diciembre).

21 Continúa el artículo 3.4. *c)* «A estos efectos, se entiende que la participación en el capital o en los derechos de voto correspondientes a acciones o participaciones es significativa cuando, por su proporción, permite a la persona que la posea tener capacidad de influencia en la persona jurídica participada».

22 El artículo 13.1 expresa que a afectos de esta Ley quedan encuadrados como sector público las siguientes entidades: a) La Administración General del Estado, las Administraciones de las comunidades autónomas, ciudades con Estatuto de Autonomía y las entidades que integran la Administración Local; b) Los organismos y entidades públicas vinculadas o dependientes de alguna Administración pública, así como aquellas otras asociaciones y corporaciones en las que participen Administraciones y organismos públicos; c) Las autoridades administrativas independientes, el Banco de España y las entidades gestoras y servicios comunes de la Seguridad Social; d) Las Universidades públicas; e) Las corporaciones de Derecho público; f) Las fundaciones del sector público (...); g) Las sociedades mercantiles en cuyo capital social la participación, directa o indirecta, de entidades de las mencionadas en las letras a), b), c), d) y g) del presente apartado sea superior al cincuenta por ciento, o en los casos en que, sin superar ese porcentaje, se encuentre respecto de las referidas entidades en el supuesto previsto en el artículo 5 del texto refundido de la Ley del Mercado de Valores, aprobado por Real Decreto Legislativo 4/2015, de 23 de octubre.

23 A la vista de la importancia numérica de las empresas con menos de 50 personas en plantilla y ante la libertad que permitía la Directiva sobre las obligaciones a imponer, Ponce y Villoria (2020) sugerían que fuesen objeto de la obligación de disponer de canales internos, aunque sus requisitos pudieran ser menores a los establecidos para las entidades del sector privado de mayor

envergadura. De hecho, también planteaban que esta minoración debería ser aplicable a los municipios pequeños por su escasez de recursos si finalmente se les terminaba requiriendo que contasen con sistemas de alerta —tal y como ha sucedido—.

24 En concreto, el artículo 10.1.*b)* hace referencia a las actividades enumeradas en las partes I.B y II del Anexo de la Directiva que están relacionadas con servicios, productos y mercados financieros, prevención del blanqueo de capitales o de la financiación del terrorismo, seguridad del transporte y protección del medio ambiente.

25 Esta obligación es mas que necesaria en el contexto actual en el que los riesgos de corrupción en los partidos políticos han terminado afectando a la credibilidad de las instituciones de nuestro sistema democrático. Por ello, hay una amplia preocupación por la integridad en los partidos políticos que abarca campos conexos como su grado de transparencia y apertura hacia la sociedad como fórmula de recuperación de la confianza ciudadana (Díez Garrido y Campos Domínguez, 2020).

26 Nótese lo contradictorio que es la exigencia de un plazo tan corto y su descompensación con lo que se ha tardado para disponer de una ley estatal en la materia, considerando que la Directiva se publicó en diciembre de 2019 y que su transposición debería haber estado hecha el 17 de diciembre de 2021.

27 La autora incide en que el proceso lógico de implantación debe tener en cuenta múltiples aspectos como el tamaño y estructura de la organización, el sector en el que desarrolla sus funciones y su modelo de funcionamiento, sus recursos y posibilidades, entre otros, considerando «los riesgos y políticas ya existentes, así como los objetivos que se pretenden conseguir» (Gutiérrez Rodríguez, 2022 p. 85). Todas estas alusiones son en definitiva las que deberían guiar cualquier proceso de implementación de actuaciones a través de un diagnóstico previo y de una planificación ordenada que es de difícil o imposible cumplimiento con el plazo tan exiguo que se da a los sujetos obligados.

28 El artículo 31 quinquies del C.P. establece como regla general que las disposiciones relativas a la responsabilidad penal de las personas jurídicas no serán aplicables «al Estado, a las Administraciones públicas territoriales e institucionales, a los Organismos Reguladores, las Agencias y Entidades públicas Empresariales, a las organizaciones internacionales de derecho público, ni a aquellas otras que ejerzan potestades públicas de soberanía o administrativas». Sin embargo, en su apartado dos si las prevé bajo algunos supuestos para las sociedades mercantiles públicas.

29 De hecho, la redacción del artículo 17 sobre la recepción de informaciones en el canal externo es menos indubitada y se complementa con el artículo 21 que establece como uno de los derechos del informante ante la autoridad estatal «formular la comunicación verbalmente o por escrito» (art. 21. 2.º).

30 Uno de los sistemas de buzón anónimo más extendidos que se puso en marcha de manera pionera en el Ayuntamiento de Barcelona y que fue acogido por las oficinas y agencias autonómicas preexistentes es GlobaLeaks (https://www.globaleaks.org/). Se trata de un software libre que permite su adaptación por cada organización y que tiene entre sus funcionalidades el envío de información de manera anónima y la posibilidad de establecer una comunicación bidireccional entre la persona informante y la entidad receptora a través de la generación de un código de acceso.

31 Nótese que Sáez Hidalgo (2021) nos ofrece pistas para conocer cuál ha sido la calificación que en el ámbito público han tenido estos pasos iniciales que se deberán contemplar en el procedimiento de gestión. En esta línea, indica que, en sede judicial, el tratamiento y seguimiento de la información había sido considerado como parte de las actuaciones previas que se establecen en el artículo 55 LPAC. Al respecto expone una sentencia del TSJ de Madrid sobre un procedimiento de investigación de la Oficina contra el Fraude y la Corrupción. El autor indicaba que esta ubicación en el artículo 55 se realizaba conforme a que la administración era la titular de una competencia, que le permite potestativamente abrir esas diligencias previas de comprobación. Sin embargo, en lo que respecta a los canales internos, ya no estaríamos hablando de actuaciones de las entidades públicas en el ejercicio de sus propias competencias, sino —como menciona el autor— en su calidad de empleadora, por lo que requeriría una aclaración del régimen aplicable para ese tipo de actuaciones que delimite su diferencia con lo establecido en el artículo 55 LPAC y también con el artículo 62 LPAC sobre la denuncia administrativa. Como podemos intuir, este interrogante no ha sido inequívocamente despejado por la Ley.

32 La Ley 2/2023 es poco afortunada al transponer algunos artículos de la Directiva que pretende imitar. Así, mientras que para los sistemas internos la Directiva fija el plazo máximo de tres meses para comunicar el resultado de las investigaciones desde que se envía el acuse de recibo —art. 9.1. *f)* Directiva—, la Ley lo hace desde que se recibe la alerta —art. 9.2. *d)*—. Esto no sería un problema porque hablamos de plazos máximos que se pueden acortar, pero lo paradójico es que cuando se hacen bien las cosas y se envía el acuse de recibo, se dispone de un plazo menor que si no se hubiera enviado, porque el mismo artículo dice: «si no se remitió un acuse de recibo al informante, [no podrá ser superior] a tres meses a partir del vencimiento del plazo de siete días después de efectuarse la comunicación», es decir, que el máximo de tres meses se fija a partir de los siete que se tenía para remitir el acuse de recibo no enviado, es decir, un plazo mayor.

33 Entre la abundante literatura que ha surgido sobre esta temática en los últimos años. Sin ánimo de exhaustividad, se pueden señalar dos libros que incluyen análisis sobre la incorporación práctica de los canales de denuncia interna. Éstos pueden servir de guía y orientación para la puesta en marcha de los sistemas de información interna, aunque se ha de advertir que se trata de textos publicados antes de la nueva Ley. Véase el libro de Beatriz García Moreno (2020) y la obra colectiva dirigida por

Núm. 24 zk./2023. Págs. 70-98 or.
ISSN: 2173-6405 e-ISSN: 2531-2103

Jordi Gimeno Beviá Belén López Donaire, M. B. (2022) que se incluyen entre las referencias bibliográficas.

34 El articulado no hace alusión a la condición que ostenta la persona informante ante los sujetos obligados a disponer de un sistema interno que formen parte del sector público, pero por aplicación del artículo 62.1 de la LPAC, la comunicación de hechos a un órgano administrativo que pudiera justificar la iniciación de oficio de un procedimiento administrativo debe entenderse como una denuncia. En estos términos se expresa el preámbulo de la Ley al indicar que «el informante por el hecho de comunicar la existencia de una infracción penal o administrativa no tiene la condición de interesado, sino de colaborador con la administración. De manera que las investigaciones que lleve a cabo (...) en el marco del Sistema interno de información del sector público (...) se inician siempre de oficio y de conformidad con el procedimiento establecido en la LPAC». Sobre este extremo sí se expresa el artículo 20.4 y 5 con relación al canal externo, al preceptuar que la presentación de una comunicación no conferirá por si sola la condición de interesado, y que las decisiones de la autoridad competente sobre las actuaciones no serán recurribles en vía administrativa o contencioso-administrativa (salvo las relativas a procedimientos sancionadores que pudieran incoarse a raíz de la comunicación). Sobre este particular, Ponce Solé (2021, p. 880 y 881) ha venido defendiendo que quienes presentan una denuncia administrativa deberían tener la consideración de interesado respecto a la decisión que se adopte sobre ella y poder impugnarla, dado que, bajo la óptica del derecho a una buena administración, quien denuncia «ostenta un derecho afectado por la tramitación correcta o no de la denuncia». Con ello, hace alusión a que el articulo 62.5 LPAC —que no confiere la condición de interesado a quien presenta una denuncia administrativa—, «se está refiriendo al subsiguiente procedimiento» que se ponga en marcha a raíz de la denuncia, pero no al relativo «al procedimiento de aceptación y decisión sobre tramitar o no la denuncia».

35 En la misma línea se pronunciaban la Oficinas y Agencias antifraude autonómicas que redactaron la propuesta de enmiendas ya mencionada. Señalaban como carencias de la independencia del canal interno la falta de previsiones sobre un proceso de selección y promoción de la persona responsable basado en el mérito; el establecimiento de garantías de inamovilidad; o su acceso a bases de datos, a información, a recursos materiales, personales y formativos; entre otras.

36 En la situación actual en la que todavía no se ha puesto en marcha la autoridad estatal, se ocasiona que los sujetos obligados de su ámbito de competencia que ya hayan nombrado sus responsables del sistema interno, no puedan dar cumplimiento a la obligación de comunicar este nombramiento en el plazo establecido de diez días (art. 8.3). No obstante, algunas comunidades autónomas están dando los pasos para determinar el organismo competente en esta materia y así se ha operado en Cataluña al atribuir estas funciones a su Oficina Antifraude autonómica a través de la Disposición Adicional 7.ª de la Ley 3/2023, de 16 de marzo, de medidas fiscales, financieras, administrativas y del sector público para el 2023.

37 En este sentido, el artículo 262 LECrim establece pena de multa y la puesta en conocimiento de superior jerárquico a efectos de responsabilidad administrativa para los empleados públicos que incumplan la obligación de denunciar delitos: «Los que por razón de sus cargos, profesiones u oficios tuvieren noticia de algún delito público, estarán obligados a denunciarlo inmediatamente al Ministerio Fiscal, al Tribunal competente, al Juez de instrucción y, en su defecto, al municipal o al funcionario de policía más próximo al sitio si se tratare de un delito flagrante». En cualquier caso, García Moreno (2020 p. 279) nos enumera algunos de supuestos adicionales que podrían dar lugar a responsabilidad —algunos ya recogidos como motivo de infracción en la Ley— como podría ser ante la ineficacia en la protección de las personas informantes, por el tratamiento «ilegítimo» de datos personales o por no hacer un seguimiento de la información.

Núm. 24 zk./2023. Págs. 70-98 or.
ISSN: 2173-6405 e-ISSN: 2531-2103