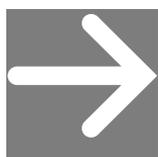


Ley reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción



Febrero 2023

¿Hablamos?

Fernando Fernández-Miranda

Socio del área de Regulación Digital de PwC Tax & Legal
fernando.fernandez-miranda.vidal@pwc.com

Rafael Manchado

Director en el área Mercantil, especialista en Corporate Governance y Compliance en PwC Tax & Legal
rafael.manchado.montero@pwc.com

Joserra Valcabado

Abogado en el área Mercantil, especialista en Corporate Governance y Compliance en PwC Tax & Legal
joserra.valcabado.pero-sanz@pwc.com

Marta Campos

Abogada en el área de Corporate M&A en PwC Tax & Legal
marta.campos.rios@pwc.com

Ignacio de Sebastián

Abogado en el área de Regulación Digital en PwC Tax & Legal
ignacio.desebastian@pwc.com

El martes 21 de febrero de 2023 se publicaba en el BOE la esperada 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 de Protección del Informante” o la “Ley”) al objeto de transponer la denominada *Directiva de Whistleblowing*.

Como continuación de la nota que elaboramos con motivo de la aprobación del correspondiente Proyecto de Ley en septiembre de 2022, en la presente nota, en primer lugar, expondremos sistemáticamente los términos en los que finalmente se tendrán que configurar los denominados **sistemas internos de información** que van a resultar de implantación obligatoria en un número relevante de entidades privadas (aquellas con más de 50 empleados) y en todas las entidades del sector público, y, en segundo lugar, destacamos otros aspectos relevantes de la reciente ley.

Con carácter preliminar, resulta importante señalar que la Ley de Protección del Informante adopta finalmente la nomenclatura, a nuestro juicio mucho más acertada, de

“informantes” en lugar de las menciones a “denunciantes” o “alertadores” que se realizaban en el Anteproyecto de Ley y en la *Directiva de Whistleblowing*.

Finalidad de la Ley

Con la Ley de Protección del Informante se persigue otorgar una protección adecuada a los informantes frente a las represalias que pudieran sufrir por el hecho de haber comunicado irregularidades o determinados incumplimientos normativos. Con esta finalidad de protección se espera que se apliquen las disposiciones de la norma a la hora de diseñar, implantar y gestionar los sistemas de información.

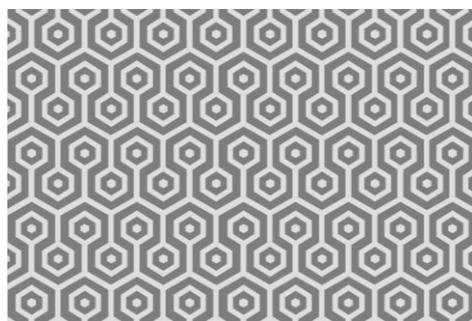
La Ley también persigue expresamente el fortalecimiento de la cultura de la información, de las infraestructuras de integridad de las organizaciones y el fomento de la cultura de la información o comunicación como mecanismo para prevenir y detectar amenazas al interés público.

Ámbito material de aplicación

Partiendo del ámbito material de aplicación de la *Directiva de Whistleblowing* que se circunscribe a las



La Ley de Protección del Informante impone nuevas obligaciones a las entidades en términos de implantación de un sistema de recepción y gestión de las comunicaciones y de la prohibición de represalias a los informantes, estableciéndose así mismo un régimen sancionador en caso de incumplimiento”.



“acciones u omisiones que puedan constituir infracciones del Derecho de la Unión Europea”, la Ley amplía el ámbito material de aplicación a las **infracciones penales y a las infracciones administrativas graves o muy graves**, considerando entre éstas, en todo caso, a las que impliquen quebranto económico para la Hacienda Pública y para la Seguridad Social. Quedan, por lo tanto, fuera de la protección de la norma las comunicaciones sobre infracciones administrativas que no sean graves y será el informante el que deba valorar ante que tipo de infracción se encuentra.

Ámbito personal de protección

Las medidas de protección de la Ley se extienden a todas aquellas personas que mantienen **vínculos profesionales o laborales** con entidades tanto del sector público como del sector privado (empleados públicos, trabajadores por cuenta ajena, autónomos, accionistas, administradores, directivos), así como a aquellas que ya han finalizado su relación profesional, voluntarios, becarios, trabajadores en período de formación o incluso personas que participan en procesos de selección.

También se extienden a las **personas que presten asistencia al informante**, a las personas de su entorno que puedan sufrir represalias, así como a las personas jurídicas propiedad del informante.

Específicamente, la Ley exige que las medidas de protección se dirijan también a los **representantes de los trabajadores** que asesoren y apoyen al informante.

Sistema interno de información

Fijado el marco de protección, tanto material como subjetivo, la Ley establece, en primer lugar, la obligación de contar con un completo sistema interno de información que se compone tanto del habitual **canal de comunicación** (lo que en la práctica se

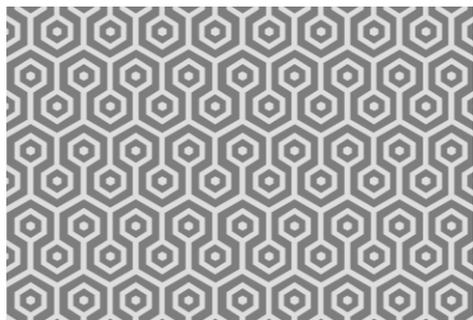
conoce como canal de denuncias o canal ético), como del **proceso de gestión y seguimiento de la información** recibida.

Estarán obligadas a disponer de dicho sistema interno de información:

- **A los tres meses desde la entrada en vigor de la Ley, esto es, el 13 de junio de 2023:**
 - Las entidades del sector público salvo los municipios de menos de 10.000 habitantes
 - Las entidades jurídicas del sector privado de 250 o más trabajadores
 - Los partidos políticos, los sindicatos, las organizaciones empresariales y las fundaciones creadas por unos y otros, siempre que reciban o gestionen fondos públicos.
- **A partir del 1 de diciembre del 2023:**
 - Las entidades jurídicas del sector privado de entre 50 y 249 trabajadores
 - Los municipios de menos de 10.000 habitantes.

En el caso de un **grupo de empresas** en los términos del artículo 42 del Código de Comercio, la sociedad dominante aprobará una política general relativa al sistema interno de información, y asegurará la aplicación de sus principios en todas las entidades que integren el grupo. En sentido contrario, las **filiales en España de grupos extranjeros** a las que le resulten de aplicación la Ley y que usen los habituales canales y procedimientos comunes en su grupo deberán cerciorarse de adaptar éstos a lo exigido por la Ley.

Con relación al sector público la ley ha extendido en toda su amplitud la obligación de contar con un sistema interno de información. En consecuencia,



han de configurar tal sistema todas las Administraciones públicas, ya sean territoriales o institucionales, las Autoridades independientes u otros organismos que gestionan los servicios de la Seguridad Social, las universidades, las sociedades y fundaciones pertenecientes al sector público, así como las Corporaciones de Derecho Público.

El órgano de administración u órgano de gobierno de cada entidad, pública o privada, es el responsable de la implantación del Sistema interno de información, **previa consulta con la representación legal de los trabajadores** y tendrá la condición de responsable del tratamiento de los datos personales.

El sistema interno de información debería utilizarse de manera preferente para canalizar la información. No obstante, **el informante puede elegir el cauce a seguir, interno o externo, según las circunstancias y los riesgos de represalias que considere.**

La configuración del sistema interno de información debe reunir determinados requisitos, entre otros, su uso asequible, las garantías de confidencialidad, las prácticas correctas de seguimiento, investigación y protección del informante, la restricción de acceso a personal no autorizado, la integración de los diferentes canales internos de información.

El sistema interno de información debe **contar con una Política que regule y publicite los principios que rigen el sistema y un procedimiento que regule la gestión de las informaciones recibidas.**

Específicamente, la Ley exige que las entidades faciliten la 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 y que, **en caso de contar con una página web, hagan constar dicha información en la página de inicio, en una sección separada y fácilmente identificable.**

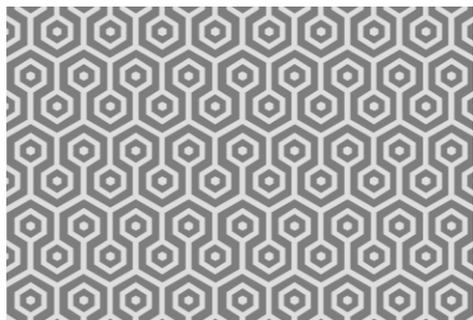
Asimismo, las entidades deben designar un **responsable del sistema** interno de información que puede ser una persona o un órgano colegiado y cuyo nombramiento, destitución o cese debe depender del órgano de administración o gobierno de la entidad. Este cargo puede recaer en el responsable de la función de cumplimiento normativo siempre que ostente un cargo directivo, en el sector privado, y, en todo caso, sea una persona con independencia y autonomía.

La gestión del sistema puede ser interna o externa a la entidad. En el caso de gestión externa la responsabilidad seguirá siendo del responsable del sistema que se haya nombrado en la entidad.

El canal de comunicación que forma parte del sistema debe permitir realizar comunicaciones por escrito o verbalmente, o de las dos formas, por medios electrónicos o incluso de forma presencial.

Las comunicaciones por el canal serán en todo caso confidenciales y éste **debe permitir también que se realicen y se tramiten comunicaciones anónimas.**

El **procedimiento de gestión de las informaciones recibidas** deberá tener el contenido mínimo previsto en la Ley y atender a los principios indicados en ésta. Entre ellos, destaca la obligación de **acuse de recibo** de la comunicación al informante, en el plazo de siete días naturales siguientes a su recepción y la fijación de un **plazo máximo para dar respuesta a las actuaciones de investigación**, que no podrá ser superior a tres meses a contar desde la recepción de la comunicación salvo casos de especial complejidad que requieran una ampliación del plazo, en



cuyo caso, este podrá extenderse hasta un máximo de otros tres meses adicionales.

Prohibición de represalias y medidas de apoyo

Se prohíben expresamente los actos constitutivos de represalia, incluidas las amenazas de represalia y las tentativas de represalia contra las personas que presenten una comunicación.

Se entiende por represalia cualesquiera actos u omisiones que estén prohibidos por la ley, o que, de forma directa o indirecta, supongan un trato desfavorable que sitúe a las personas que las sufren en desventaja particular con respecto a otra en el contexto laboral o profesional, solo por su condición de informantes.

La Ley incorpora una lista a título ejemplificativo de las acciones que se pueden considerar represalias.

En los procedimientos laborales corresponderá a la entidad que haya tomado una medida perjudicial probar que esa medida se basó en motivos debidamente justificados no vinculados a una comunicación o revelación pública.

Asimismo, se prevén determinadas medidas de apoyo a las que podrán acceder los informantes, tales como, asesoramiento público y gratuito sobre procedimientos y recursos disponibles, asistencia efectiva por parte de las autoridades en relación con la protección frente a represalias o, en su caso, apoyo financiero o psicológico.

Protección a las personas afectadas

Aquellas personas a las que se refieran los hechos relatados en la comunicación mantienen todos sus derechos de tutela judicial y defensa, de acceso al expediente, de confidencialidad y reserva de identidad y la presunción de inocencia.

Régimen sancionador

La Ley establece un preciso régimen sancionador, considerando infracciones, entre otras, cualquier actuación que suponga una efectiva limitación de los derechos y garantías previstos introducida a través de contratos o acuerdos a nivel individual o colectivo, cualquier intento o acción efectiva de obstaculizar la presentación de comunicaciones o de impedir, frustrar o ralentizar su seguimiento, incluida la aportación de información o documentación falsa por parte de los requeridos para ello, la adopción de cualquier represalia, o la vulneración de las garantías de confidencialidad y anonimato, entre otras.

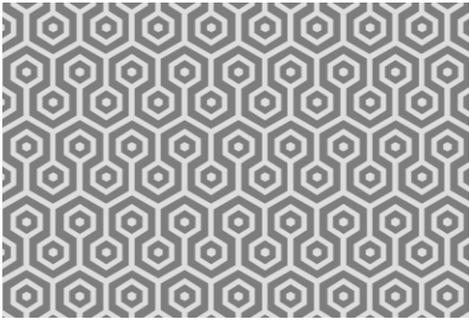
El órgano sancionador será la Autoridad Independiente de Protección del Informante o el organismo homónimo en el ámbito autonómico en función del ámbito de la infracción.

Las sanciones por la comisión de infracciones **se pueden imponer tanto a la entidad infractora, pública o privada, como a los órganos internos responsables.**

Las sanciones a personas jurídicas pueden llegar hasta el millón de euros y hasta los trescientos mil euros para personas físicas para las muy graves, como por ejemplo, en el caso de incumplimiento de la obligación de disponer del propio sistema interno de información en los términos exigidos por la norma.

Especialidades en materia de protección de datos

La Ley de Protección del Informante establece un régimen específico en materia de protección de datos personales dada la relevancia que éstos supondrán en la gestión de las comunicaciones de infracciones, de forma que modifica el artículo 24 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y



garantía de los derechos digitales para hacer una referencia al contenido de la propia Ley.

Con respecto a la base legitimadora, la Ley establece una presunción de licitud, aclarando que los tratamientos de datos personales realizados en aplicación de la misma se entenderán amparados en el cumplimiento de una obligación legal siempre y cuando la entidad esté obligada a disponer de un sistema interno de información y en los supuestos de canales de comunicación externos.

Para los casos en los que disponer de un sistema de información no fuese obligatorio o cuando el tratamiento se derivase de una revelación pública, el tratamiento se presumirá lícito en la medida en la que se considera que resulta necesario para el cumplimiento de una misión realizada en interés público.

Adicionalmente, se establece una presunción de licitud para el tratamiento de categorías especiales de datos personales amparándolo en el interés público esencial.

Además de facilitar información adecuada y suficiente a los informantes y a quienes lleven a cabo una revelación pública en los términos establecidos en el Reglamento General de Protección de Datos, será necesario que, expresamente, se informe a los interesados de que su identidad será reservada y que no se comunicará a las personas a las que se refieren los hechos revelados ni a terceros.

Teniendo en consideración lo anterior, en el supuesto de que los afectados por los hechos relatados ejercieran su derecho de acceso, se debería tener presente que el nombre de los informantes es un dato que nunca debería facilitarse. Igualmente, en el caso de que el afectado ejerciese su derecho de oposición, se presumirá, salvo prueba en contrario, que existen

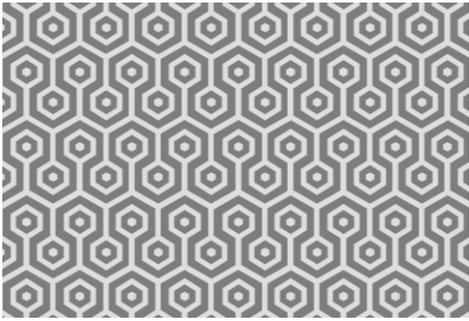
motivos legítimos imperiosos que legitiman el tratamiento de sus datos.

Otra medida con la que se pretende proteger a los informantes es limitando el acceso a los datos contenidos en el sistema de información a las personas que, atendiendo a sus competencias y funciones dentro de la entidad, resulten estrictamente necesarias. En este sentido, el legislador ha incluido una lista cerrada de personas que podrán tener acceso a los datos aunque matiza que los datos podrán también ser comunicados a personas distintas de las incluidas en esa lista o, incluso, a terceros cuando así resulte necesario para la adopción de medidas correctoras o la tramitación de procedimientos tanto sancionadores como penales.

Sobre la conservación de los datos personales, se establece que los mismos solo podrán ser almacenados en el sistema de información durante el tiempo que resulte imprescindible para decidir sobre la procedencia de iniciar o no una investigación.

En cualquier caso, cuando transcurran tres meses desde la recepción de la comunicación sin que se hubiesen iniciado actuaciones de investigación se deberán suprimir los datos personales a menos que el objetivo de conservarlos sea dejar evidencia del funcionamiento del sistema, en cuyo caso los datos deberán ser anonimizados

Por último, resulta relevante poner de manifiesto la incongruencia existente entre el Preámbulo de la Ley y su articulado en relación con el Delegado de Protección de Datos ("DPD"). A este respecto, si bien en el propio Preámbulo se exige a las entidades obligadas a disponer de un sistema interno a contar con un DPD, el artículo 34 de la Ley únicamente exige nombrar un DPD a la Autoridad Independiente de Protección del Informante, A.A.I., y las autoridades independientes que en su caso se constituyan.



Canal externo de información de la Autoridad Independiente de Protección del Informante y revelación pública

Ante una acción u omisión que conlleve una infracción de las previstas en la Ley, el informante podrá optar por informar a la Autoridad Independiente de Protección del Informante o a las autoridades u órganos autonómicos correspondientes, ya sea directamente o previa comunicación a través del correspondiente canal interno. En última instancia, el informante podrá hacer una relevación pública de la infracción de la que ha tenido conocimiento, tras haber realizado la comunicación primero por canales internos y externos, o directamente por canales externos, sin que se hayan tomado medidas apropiadas al respecto en el plazo establecido y entienda que se da una situación de peligro inminente para el interés público, entre otros.

Modificaciones de otras normas

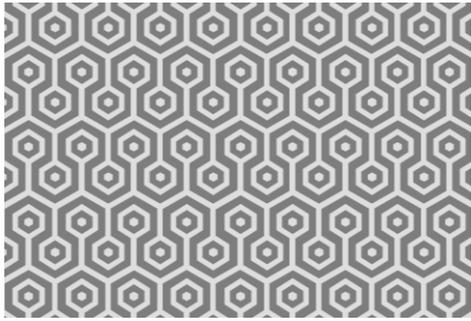
La Ley modifica, entre otras, las siguientes normas:

- La *Ley de asistencia jurídica gratuita* a los efectos de incorporar a los informantes protegidos por esta ley como beneficiarios de dicha asistencia.
- La *Ley de Defensa de la Competencia* al objeto de regular el sistema de comunicación de infracciones de dicha ley mediante el canal externo de la CNMC.
- La *Ley Orgánica de Protección de Datos Personales* al objeto de hacer una referencia expresa a que los tratamientos de datos personales en el contexto de los sistemas de información se registrarán por lo establecido en la propia Ley de Protección del Informante.

En cualquier caso, cuando transcurran tres meses desde la recepción de la comunicación sin que se hubiesen iniciado actuaciones de investigación se deberán suprimir los datos personales a menos que el objetivo de conservarlos sea dejar evidencia del funcionamiento del sistema, en cuyo caso los datos deberán ser anonimizados. Por último, resulta relevante poner de manifiesto la incongruencia existente entre el Preámbulo de la Ley y su articulado en relación con el Delegado de Protección de Datos ("DPD"). A este respecto, si bien en el propio Preámbulo se exige a las entidades obligadas a disponer de un sistema interno a contar con un DPD, el artículo 34 de la Ley únicamente exige nombrar un DPD a la Autoridad Independiente de Protección del Informante, A.A.I., y las autoridades independientes que en su caso se constituyan.

Canal externo de información de la Autoridad Independiente de Protección del Informante y revelación pública

Ante una acción u omisión que conlleve una infracción de las previstas en la Ley, el informante podrá optar por informar a la Autoridad Independiente de Protección del Informante o a las autoridades u órganos autonómicos correspondientes, ya sea directamente o previa comunicación a través del correspondiente canal interno. En última instancia, el informante podrá hacer una relevación pública de la infracción de la que ha tenido conocimiento, tras haber realizado la comunicación primero por canales internos y externos, o directamente por canales externos, sin que se hayan tomado medidas apropiadas al respecto en el plazo establecido y entienda que se da una situación de peligro inminente para el interés público, entre otros.



Modificaciones de otras normas

La Ley modifica, entre otras, las siguientes normas:

- La *Ley de asistencia jurídica gratuita* a los efectos de incorporar a los informantes protegidos por esta ley como beneficiarios de dicha asistencia.
- La *Ley de Defensa de la Competencia* al objeto de regular el

sistema de comunicación de infracciones de dicha ley mediante el canal externo de la CNMC.

- La *Ley Orgánica de Protección de Datos Personales* al objeto de hacer una referencia expresa a que los tratamientos de datos personales en el contexto de los sistemas de información se registrarán por lo establecido en la propia Ley de Protección del Informante.