REVISTA
DE DERECHO, EMPRESA Y SOCIEDAD
(REDS)

Número 22 y 23 , Época II, 2023

ISSN: 2340-4647

IURE LICET ABOGADOS

Dykinson, S.L.

REDACCIÓN Y ADMINISTRACIÓN

Revista de Derecho Empresa y Sociedad (REDS).

IURE LICET ABOGADOS (Área de Investigación)

Bilbao, C/ Gran Vía, 55, 1º Izda

E-mail iurelicet@iurelicet.com

ADQUISICIÓN Y SUSCRIPCIONES

Dykinson, S.L.

Suscripción versión electrónica (Revista en PDF).

Compra directa a través de nuestra web:

www.dykinson.com/derechoempresaysociedad

EL ESTATUTO DE PROTECCIÓN DEL INFORMANTE Y DERECHOS FUNDAMENTALES CONCERNIDOS SEGUN LA LEY 2/2023, DE 20 DE FEBRERO

Ana María Gil Antón
Doctora en Derecho. Delegada de Protección de datos certificada esquema AEPD
Profesor Tutor Master de Acceso Abogacía de la UNED

Fecha de recepción: 20 de septiembre de 2023
Fecha de aceptación: 27 de octubre de 2023

RESUMEN: Con la aprobación de la ley 2/2023, de 20 de febrero, se incorpora al Derecho español la Directiva (UE) 2019/1937 del Parlamento Europeo y del Consejo, de 23 de octubre de 2019, para proteger a los informantes y establecer las normas mínimas de los canales de información, porque se considera, que es "más efectivo" que la información sobre prácticas irregulares se conozca por la propia organización para corregirlas o reparar lo antes posible los daños, fijándose una serie de garantías para las personas informantes que realicen las denuncias, un **verdadero Estatuto de protección del informante, ,** sin olvidar las propias garantías que ostentan las personas que pueden quedar afectadas con la denuncia de hechos tipificados como delitos e infracciones graves o muy graves. En el presente estudio se procederá a un análisis de esas garantías con las que cuentan los informantes, con objeto evitar represalias y salvaguardar tanto la aplicación del Derecho fundamental a la defensa y la tutela judicial efectiva, así como el de la protección de datos, previstos ambos en la Constitución española. A los tres meses desde la entrada en vigor de la Ley, esto es, **el 13 de junio de 2023**, se estableció la obligatoriedad para las entidades del sector público salvo los municipios de menos de 10.000 habitantes, para las entidades jurídicas del sector privado de 250 o más trabajadores, así como para los partidos políticos, los sindicatos, las organizaciones empresariales y las fundaciones creadas por unos y otros, siempre que reciban o gestionen fondos públicos. Pero es a partir del **1 de diciembre del 2023** cuando quedarán obligadas las entidades jurídicas del sector privado de entre 50 y 249 trabajadores, al igual que los municipios de menos de 10.000 habitantes.

ABSTRACT: With the approval of ACT 2/2023, of February 20, Directive (EU) 2019/1937 of the European Parliament and of the Council, of October 23, 2019, is incorporated into Spanish Law, to protect informants and establish the minimum standards of the information channels, because it is "more effective" that the information about irregular practices be known by the organization itself in order to correct them or repair the damage as soon as possible, being notable the fact that that a series of guarantees are established for the informants who make the complaints, a true Statute of protection of the informant without forgetting the guarantees held by the people who may be affected by the report of events classified as serious or very serious crimes and infractions. . In this study, an analysis will be made of those guarantees that informants have, in order to avoid reprisals and safeguard both the application of the fundamental right to defense and effective judicial protection, as well as that of data protection, provided both in the Spanish Constitution. Three months after the entry into force of the Law, that is, on June 13, 2023, the obligation was established for public sector entities except municipalities with less than 10,000 inhabitants, for legal entities in the private sector of 250 or more workers, as well as for political parties, unions, business organizations and foundations created by them, as long as they receive or manage public funds. But it is as of December 1, 2023 that legal entities in the private sector with between 50 and 249 workers will be obligated, as will municipalities with less than 10,000 inhabitants.

PALABRAS CLAVE: prácticas irregulares, canales de Información, garantías de Protección

KEYWORS: irregular practices, information channels, protection guarantees

1. INTRODUCCIÓN.

Cumplir ejemplar y diligentemente con la legalidad vigente, actuando siempre desde un enfoque preventivo y de minimización de riesgos -tanto económicos, como sociales, ambientales y fiscales-, y garantizar y promover un comportamiento societario y corporativo ejemplar, a través de la adopción de las mejores prácticas de gobierno corporativo, transparencia, integridad y ética empresarial, son valores que en general tanto el sector público como el privado han de cumplir. Se trata de establecer mecanismos y medios que generen credibilidad y confianza en los ciudadanos y el público en general. No obstante, se ha constatado que ello no es siempre así, y las practicas no éticas, las corruptelas y los ilícitos siguen produciéndose en el ámbito de las Administraciones públicas como en el

empresarial, tanto a nivel nacional, como comunitario, y por consiguiente se requiere de un sistema que aliente a los informantes para la denuncia de estas prácticas, lo que no está exento de que éstos sufran represalias, cuestión que se ha constatado que requiere de una regulación con objeto de que estas las personas que denuncian o alertan puedan quedar protegidas.

La Directiva (UE) 2019/1937, del Parlamento Europeo y del Consejo de 23 de octubre, Directiva Whistleblowing", ha pretendido reforzar en el ámbito de los estados miembros la cultura de cumplimiento de las entidades públicas y privadas y establecer unas normas mínimas comunes con el propósito de garantizar la protección de las personas que denuncian tales prácticas. La finalidad de 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, con la que se incorporó al derecho español dicha Directiva, es la de proteger a las personas que en un contexto laboral o profesional detecten infracciones penales o administrativas graves o muy graves y las comuniquen mediante los mecanismos regulados en la misma, esto es los sistemas de información y sus canales de denuncia internos. No obstante, la nueva ley también prevé un canal externo, a través de una nueva Autoridad de control que se crea, la Agencia Independiente de Protección del Informante A.A.I., aunque en la interpretación de la ley, parece que el cauce más adecuado sería la denuncia interna.

La Ley 2/2023, no hace sino cumplir una obligación de nuestra pertenencia a la Unión Europea y se enmarca en un contexto internacional de protección del denunciante, que se ha de entender, que se extiende más allá de las fronteras de la Unión, como se recoge en Convenciones internacionales, como la de Nueva York. Trata de fijar mecanismos e instrumentos para proteger a quienes informen sobre las infracciones del Derecho de la Unión previstas en la Directiva, abarcando también las infracciones penales y administrativas graves y muy graves de nuestro ordenamiento jurídico.

Con carácter general, la norma determina que cada una de las denominadas "*personas jurídicas obligadas*" en la misma ha de cumplir con la obligación de disponer de su propio sistema interno de información (art. 4.2) y su canal del informante, que afecta tanto a las empresas del sector privado como al sector público. Este deber únicamente se excepciona para las entidades del sector privado que tengan menos de cincuenta trabajadores y no intervengan en los servicios previstos en el artículo 10.1.b) de la Ley, pero no para las personas jurídicas del sector público (artículos 13 y 14.3), que se encuentran todas ellas obligadas a contar con estos sistemas. El legislador español al incorporar la norma al ordenamiento jurídico, ha hecho uso de forma parcial de la opción de exonerar a las entidades privadas de menos de 50 empleados, de disponer de un sistema interno de información, si bien debe tenerse en cuenta, que el propio art.10.2 dispone que las entidades no obligadas puedan establecer dicho sistema de información interno, que en todo caso, debe ajustarse a las previsiones legales, en casos de existir.

Frente a lo previsto para la entrada en vigor de esta norma en relación con el sector público y empresas privadas de más de 250 trabajadores- respecto a la necesidad de fijación de los canales de denuncia y sistemas de información- que se fijó a los tres meses de su entrada en vigor[1], esto es el pasado 13 de junio, sin embargo, para aquellas privadas que tuvieran

[1]Disposición Transitoria Segunda. Plazo máximo para el establecimiento de Sistemas internos de información y adaptación de los ya existentes. 1. Las Administraciones, organismos, empresas y demás entidades obligadas a contar con un Sistema interno de información deberán implantarlo en el plazo máximo de tres meses a partir de la entrada en vigor de esta ley. 2. Como excepción, en el caso de las entidades jurídicas del sector privado con doscientos cuarenta y nueve trabajadores o menos, así como de los municipios de menos de diez mil habitantes, el plazo previsto en el párrafo anterior se extenderá hasta el 1 de diciembre de 2023.
3. Los canales y procedimientos de información externa se regirán por su normativa específica resultando de aplicación las disposiciones de esta ley en aquellos aspectos en los que no se adecúen a la Directiva (UE) 2019/1937 del Parlamento Europeo y del Consejo, de 23 de octubre de 2019. Dicha adaptación deberá producirse en el plazo de seis meses desde la entrada en vigor de esta ley. En estos

entre 50 y 249 empleados se ha determinado que deberán contar con dichos sistemas en fecha de 1 de diciembre de 2023, según dispone la Disposición Transitoria Segunda.

Por su parte, respecto de los Grupos de sociedades la regulación se dispone en el art.11 de la Ley indicando que "*En el caso de un grupo de empresas…..(…),la sociedad dominante aprobará una política general relativa al Sistema interno de información a que se refiere el artículo 5 y a la defensa del informante, y asegurará la aplicación de sus principios en todas las entidades que lo integran, sin perjuicio de la autonomía e independencia de cada sociedad, subgrupo o conjunto de sociedades integrantes que, en su caso, pueda establecer el respectivo sistema de gobierno corporativo o de gobernanza del grupo*,…(..)", es decir en el supuesto de los grupos de sociedades podríamos entender de aplicación la Teoría de la Organización), por cuanto las actividades relacionadas con la función de cumplimiento normativo o con el *"compliance"* se consideran "*actividades de gobierno*" o de gobernanza y vertebran, en el caso de grupos, a todos sus integrantes. El derecho de sociedades mercantiles las incluye en la categoría de "gobierno corporativo" o de "buen gobierno societario", y en ese mismo grupo de actividades habrá que incluir las actuaciones vinculadas a la Ley 2/2023, en la medida en que sigue la misma finalidad, al enmarcarlas en el ámbito del fortalecimiento de la cultura de información, integridad y cumplimiento, como destaca su artículo 1.2.

En este sentido, se pronuncia positivamente la Comisión Europea, en relación a mecanismos a nivel de grupo, en la interpretación que hace del alcance de la Directiva (UE) 2019/1937 en dos cartas interpretativas de 2021, emitidas en respuesta a varias consultas de *Business Europe*[2]. Así en la carta de 2 de junio de 2021 se afirma que "*basándose en el apartado 6 del artículo 8, cuando en un determinado grupo empresarial los programas de cumplimiento se organicen a nivel de la sede central, podría ser compatible con la Directiva que una filial se beneficie de la capacidad de investigación de su sociedad matriz siempre que se den determinados requisitos*"[3]. Ahora bien, en todo caso, estos instrumentos que se permiten para los grupos de sociedades serán válidos en la medida, como señala la Comisión, que sean los propios informantes los que libre y voluntariamente decidan utilizarlos, por considerar que pueden tratar de manera más efectiva la infracción comunicada y que no hay riesgo de represalia. Hay que recordar que la voluntariedad es un principio esencial en el esquema de la Ley 2/2023 para los sistemas internos, hasta el punto de que la Ley ni siquiera impone como obligatoria la existencia de una denuncia interna. En todo caso, los mecanismos alternativos o complementarios no conllevan ni pueden implicar que haya una minoración o relajación de las obligaciones específicas que incumben a las personas y entidades obligadas a tener su propio sistema interno, ni puede impactar sobre el nivel de exigencia de los sistemas internos de información preceptivos.

Aunque las cartas interpretativas de la Comisión Europea dan respuesta a planteamientos sobre grupos de empresas del sector privado, sus planteamientos están basados en las reglas generales de la Directiva. Como se deduce de la carta interpretativa de la Comisión Europea[4] de 02.06.2021, una política empresarial que infunda confianza en la función de denuncia de irregularidades del grupo, posiblemente acompañada de una buena política de

---

supuestos, el informante gozará de la protección establecida en esta ley siempre que la relación laboral o profesional en cuyo contexto se produzca la infracción, se
rija por la ley española y, en su caso, adicionalmente de la protección establecida en la normativa específica

[2] (identificadas como Brussels, 29.06.2021. JUST/C2/MM/rp/ (2021)4667786 y Brussels, 02.06.2021 JUST/C2/MM/rp/ (2021)3939215)

[3] 1) la empresa filial sea de tamaño medio (tenga entre 50 y 249 trabajadores) 2) existan y sigan existiendo canales de información a nivel de la filial 3) se facilite información clara a los denunciantes sobre el hecho de que una
persona/departamento designado a nivel de la sede central estaría autorizado a acceder a la denuncia (con el fin de llevar a cabo la investigación necesaria), y el denunciante tenga derecho a oponerse a ello y a solicitar que la conducta denunciada sólo se investigue a nivel de la filial; 4) se adopte cualquier otra medida de seguimiento y se informe al denunciante a nivel de la filial

[4] JUST/C2/MM 2.06.2021

información que dé a conocer su disponibilidad y anime a los denunciantes a informar a las funciones centrales de denuncia de irregularidades del grupo, puede dar lugar a que los denunciantes tiendan a elegir informar allí. No obstante, la posibilidad de informar a la filial en la que trabaja el denunciante debe seguir estando siempre efectivamente disponible.

Podemos por tanto concluir, que en el ámbito privado, siguiendo la previsión de la Directiva, estarán obligadas a configurar un sistema interno de información todas aquellas empresas que tengan más de cincuenta trabajadores.

Por tanto, en los grupos de empresas, de acuerdo con lo dispuesto en el art.11 de la Ley, será la sociedad dominante la que pueda implantar los principios y políticas que inspiren la organización del sistema para la adecuada organización y coordinación de los canales de denuncia en cada una de las entidades que forman parte de aquel. Y por su parte, siendo consciente la ley, del coste que esta nueva obligación pueda generar en las empresas, permite que aquellas que, superando la cifra de cincuenta trabajadores cuenten con menos de doscientos cincuenta, puedan compartir medios y recursos para la gestión de las informaciones que reciban, quedando siempre clara la existencia de canales propios en cada empresa, y ello para las empresas privadas, de conformidad con lo previsto en el art.12.

En los términos expuestos, en relación con las personas obligadas a disponer de un sistema interno de información, el artículo 5.2 de la Ley prevé no obstante la posibilidad de distintas fórmulas de gestión, aunque estás deberán respetar los principios y criterios de los artículos 4 a 15. Entre estas fórmulas de gestión del sistema interno de información se admite expresamente la gestión por tercero externo en su artículo 6, aunque en dicho supuesto dicha gestión del sistema, se ha de considerar limitada a la recepción de informaciones, sin perjuicio de posibles interpretaciones a la luz de los preceptos de la Ley.

En definitiva, la gestión del sistema interno se puede llevar a cabo dentro de la propia entidad obligada, directamente o empleando los medios compartidos previstos en los artículos 12 y 14, o a través, con ciertas condiciones, de un tercero externo (artículos 6.1 y 15 de la Ley 2/2023). Ahora bien, en materia de externalización por un tercero, el régimen previsto para el sector privado no es el mismo que para el público (artículo 15), determinándose en los casos de externalización una limitación a la propia responsabilidad, por cuanto en su apartado 3 se refiere a que *"la gestión del sistema de información por un tercero, no podrá suponer un menoscabo de las garantías y requisitos que para dicho sistema establece la ley, ni una atribución de la responsabilidad sobre el mismo en persona distinta del Responsable del sistema a que se hace mención en su artículo 8."*. Es decir, en cuanto a la externalización del sistema interno de información, se establecen dos cautelas: por un lado, el respeto absoluto a los principios de independencia, confidencialidad, protección de datos y secreto de las comunicaciones; y, por otro, que no suponga un menoscabo de las garantías previstas ni una alteración de la responsabilidad, que seguirá recayendo en el responsable del sistema de información, que de acuerdo con la Ley deberá ser designado por el órgano de administración u órgano competente de la entidad u organismos correspondiente.

2. PRINCIPIOS DE GARANTÍA EN LOS SISTEMAS INTERNOS DE INFORMACIÓN

De acuerdo con el objeto de la Ley 2/2023, se ofrecen una serie cauces adecuados tanto a las Administraciones y personas públicas y privadas de poner en su conocimiento no solo posibles actuaciones de corrupción, hechos tipificados como delitos, e infracciones graves y muy graves, sino también y simultáneamente, ofrecer una serie de garantías adecuadas frente a las represalias que puedan sufrir las personas físicas que informen, a través de los procedimientos previstos en la misma. Uno de los objetivos esenciales que busca la Ley, es la efectividad del funcionamiento de los sistemas internos de información y de la protección que debe conferir al informante.

La necesidad de hacer operativo el principio de la efectividad del sistema es una de las mayores pretensiones de la regulación de la Directiva, especialmente en la implantación de unos canales de denuncia efectivos, confidenciales y seguros, tal como se hace constar en los considerandos 3 y 47 y el artículo 7.2 de la misma, al exigir la aplicación de dichos principios en los canales de denuncia interna, "*siempre que se pueda tratar la infracción internamente de manera efectiva*". Y este mismo principio se traslada a la regulación de la Ley 2/2023. En efecto, en su artículo 4, prevé que el sistema interno de información sea el cauce preferente para informar sobre las acciones u omisiones previstas en su ámbito objetivo (art. 2), para el art. 5.2.e), disponer que el sistema interno de información deberá "*Garantizar que las comunicaciones presentadas puedan tratarse de manera efectiva dentro de la correspondiente entidad u organismo con el objetivo de que el primero en conocer la posible irregularidad sea la propia entidad u organismo",* es decir la entidad que pudiera estar afectada.

No obstante, como analizaremos, nuestra norma no solo va más allá en cuanto al objeto de la propia Directiva, ampliando los supuestos de posible información, sino también fijando una serie de condiciones que tratan de preservar los derechos fundamentales que se pudieran ver concernidos procedentes de la información y de los informantes, como la tutela judicial efectiva, derecho de defensa y presunción de inocencia, además de la protección de datos y el derecho al honor y, estableciendo todo un Estatuto de protección para el denunciante, pero sin obviar, como veremos, las normas del proceso penal y las personas que pudieren resultar afectadas, tanto personas físicas como jurídicas.

En consecuencia, para una adecuada interpretación que pueda darse a los preceptos de la Ley 2/2023 deberá también considerarse la necesidad de garantizar no sólo la efectividad del sistema interno de información o sus elementos integrantes, sino el respeto de los principios que deben presidir el tratamiento de la información en los sistemas, como el de transparencia, confidencialidad, seguridad vinculados con las garantías que se otorgan a los informantes, de tal manera que exige una serie de requisitos, destacando no sólo que se debe permitir a todas las personas referidas en el art.3 de la Ley, la comunicación de infracciones, sino que en su art. 5.2.b se indica que ha de *" estar diseñado, establecido y gestionado de forma segura, de modo que se garantice la confidencialidad y la identidad del informante y de cualquier tercero mencionado en la comunicación y de las actuaciones que se desarrollen en la gestión y tramitación de la misma, así como la protección de datos, impidiendo el acceso de personal no autorizado*", y fijándose en el art.9.2 las condiciones y requisitos que habrán de cumplir dichos canales y sistemas de información.

3. PERSONAS PROTEGIDAS FRENTE A LAS REPRESALIAS

Con respecto a las personas informantes que están protegidas frente a posibles represalias, de acuerdo con el artículo 3 de la Ley 2/2023, son todas aquellas que tienen vínculos profesionales o laborales con entidades tanto del sector público como del sector privado, aquellas que ya han finalizado su relación profesional, voluntarios, trabajadores en prácticas o en período de formación, personas que participan en procesos de selección, y aquellos cuya relación laboral todavía no haya comenzado, cuando la información sobre infracciones haya sido obtenida durante el proceso de selección o de negociación precontractual, al igual que a las que prestan asistencia a los informantes, o a las personas de su entorno que puedan sufrir represalias, así como a las personas jurídicas propiedad del informante, entre otras .En este sentido, se expresa dicho precepto, que se refiere a *"los informantes que trabajen en el sector privado o público y que hayan obtenido información sobre infracciones en un contexto laboral o profesional",* concepto que comprende, en todo caso, a los empleados públicos o trabajadores por cuenta ajena[5],

[5] Artículo 3.3 de la ley 2/2023 "Y a sus representantes en el ejercicio de sus funciones de asesoramiento y apoyo al informante".

autónomos, accionistas, partícipes y miembros del órgano de administración, dirección o supervisión de una empresa, y cualquier persona que trabaje para o bajo la supervisión y la dirección de contratistas, subcontratistas y proveedores.

Además las medidas de protección se aplican también, en su caso, a las personas físicas que en el marco de una organización en la que preste servicios el informante, asistan al mismo en el proceso; a las personas físicas relacionadas con el informante y que puedan sufrir represalias, como compañeros de trabajo o familiares del informante y a las personas jurídicas, 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, al igual que se aplicará a los denunciantes cuando comuniquen o revelen públicamente información sobre infracciones obtenida en el marco de una relación laboral ya finalizada, tal como se contiene en el art.4 de la Directiva.

En dicho ámbito de sujetos obligados se incluye, en consecuencia, tanto a los empresarios personas físicas, como a las personas jurídicas**,** y dentro de estas con independencia del tipo societario o asociativo o fundaciones que adopten. En este sentido se incluirían las entidades sin personalidad jurídica como comunidades de bienes, herencias yacentes, sociedades irregulares o en formación, sociedades ocultas y Uniones Temporales de empresas[6]. También se incluyen los partidos políticos, los sindicatos, organizaciones empresariales y las fundaciones creadas por unos u otros, siempre que reciban o gestionen fondos públicos.

4. GARANTÍAS Y MEDIDAS DE PROTECCIÓN DEL INFORMANTE

La finalidad de la Ley 2/2023, como venimos diciendo, es clara siguiendo la línea marcada por la Directiva, de una parte alentar las informaciones sobre ilícitos o actuaciones de corrupción, pero al tiempo establecer una serie de condiciones de protección para evitar las represalias al informante, regulando dos condiciones, que las personas que revelen infracciones han de tener motivos razonables para considerar que están ofreciendo una información veraz, y que la denuncia se canalice por alguno de los mecanismos fijados en la Ley, bien canal interno o canal externo de la Autoridad Independiente de Protección del Informante o del correspondiente órgano u organismo de la Comunidad Autónoma, de existir, o acudiendo a la revelación pública, tal como señala el art.35, que parte de la buena fe del informante, ya que se ampara a "*aquellas personas que mantienen una actitud cívica y de respeto democrático*", en el ámbito de las vías de comunicación previstas en la Ley, lo que no excluiría las denuncias ante la Policía o ante la Fiscalía o un Juez, situación ante las que el denunciante no tendría las garantías de la Ley 2/2023, pero sí las que le brinda la ley a los testigos en el procedimiento penal.

En realidad el espíritu de la Ley 2/2023, es fijar una serie de garantías del informante que tratan de hacerse posible con la gestión de los sistemas de información y canales de denuncia, de una parte, con el respeto al derecho fundamental a la protección de sus datos personales, y de otra garantizar y evitar las eventuales represalias, a través del establecimiento de mecanismos que al tiempo que traten de prevenir y detectar actuaciones irregulares[7], establezcan medidas de garantía que habrán de respetarse en la gestión de comunicaciones y tramitaciones, el derecho fundamental a la protección de datos**,** el derecho al honor, a la tutela judicial efectiva y el derecho de defensa**,** así como el deber de seguridad y confidencialidad, con la preservación de la identidad del informante al denunciado y terceros, o a través del anonimato. Por su parte, en cuanto a la gestión de las

[6]Art.10 b y c de la Ley 2/2023

[7] Guidelines on processing personal information within a whistleblowing procedure, publicadas en el mes de julio de 2016 y actualizadas en diciembre de 2019. Disponible en https://edps.europa.eu/dataprotection/our-work/our-work-by-type/guidelines_en.

informaciones se establece así mismo, otra serie de principios en el ámbito de la protección de datos como la minimización de los datos, los plazos de conservación de la información, el derecho de información y, en definitiva, un tratamiento de los datos del denunciante y de terceros afectados en las informaciones, acordes con la normativa de protección de datos, cuestiones sobre las que ya se han pronunciado tanto el Consejo del Poder Judicial[8], como la propia AEPD[9] en diversos informes.

La pretensión de la Ley fijar unos principios, garantías y límites en la aplicación de los sistemas de *compliance,* y, por tanto en relación con la responsabilidad penal de las personas jurídicas[10] y su normativa reguladora,[11]al considerar lo más recomendable, que sea la propia organización donde se producen las irregularidades la que depure, de forma temprana, transparente y con pleno respeto de los derechos del informante y de los afectados por la denuncia, estos comportamientos ilícitos o prácticas indeseables, si bien prohibiendo las represalias, entendidas como cualesquiera actos u omisiones que esté 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 o por haber hecho una revelación pública(art.36.2 de la Ley, mencionando a título enunciativo una relación de conductas, y contemplando una serie de medidas de protección frente a eventuales represalias (art.36.5, 38 y 39 de la Ley).

Pero con carácter previo, y para garantizar que no se produzcan dichas conductas de represalia por identificación del denunciante, el artículo 33.2 de la Ley 2/2023, exige que los sistemas internos de información, los canales externos y quienes reciban revelaciones públicas deberán contar con medidas técnicas y organizativas adecuadas para preservar la identidad y garantizar la confidencialidad de los datos correspondientes a las personas afectadas y a cualquier tercero que se mencione en la información suministrada, especialmente la identidad del informante en caso de que se hubiera identificado. Ello incide en el cumplimiento reforzado de los principios de confidencialidad e integridad, debiendo implementar medidas de seguridad apropiadas en los sistemas de *whistleblowing*, que han de ser suficientemente sólidas como para impedir no solo brechas de seguridad, sino accesos no autorizados a los canales de denuncias, con lo que se vulneraría la confidencialidad y la seguridad, pudiendo facilitar dichas represalias.

Otro de los principios a tener en cuenta en la tramitación, es el de la conservación de los datos, que no deben conservarse "más tiempo del necesario para los fines del tratamiento"(art. 5.1 e) del RGPD, prescribiendo los artículos 26.2 y 32 de la Ley 2/2023, que los datos que pudieren ser objeto de tratamiento y almacenamiento, podrán conservarse en el sistema de información únicamente durante el tiempo imprescindible para la procedencia del inicio de una investigación sobre los hechos informados, y en consecuencia sólo mientras sea necesario para la tramitación de su denuncia, investigación, informe y por

[8] Informe del Consejo del Poder judicial de 26 de mayo de 2022 sobre el anteproyecto de Ley reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción por la que se transpone la directiva (UE) 2019/1937 del parlamento europeo y del consejo, de 23 de octubre, relativa a la protección de las personas que informen sobre infracciones del derecho de la unión

[9]0054/2023 Informe Gabinete Jurídico de la AEPD.

[10]Artículos 31 bis. 2, 1ª y 2ª, 31 bis.5, 4ª y 31 quater d) del Código Penal, introducidos por la Ley Orgánica 1/2015, de 30 de octubre.

[11] Vazquez de Castro, E; "La doble faceta de la protección de datos personales en los sistemas de compliance". Revista Aranzadi de Derecho y Nuevas Tecnologías, numero 59(2022) "El compliance o cumplimiento normativo es un mecanismo preventivo que sirve para liberar de responsabilidad a las personas jurídicas. Uno de los aspectos importantes que deben tenerse en cuenta a la hora de prevenir incumplimientos es el derecho a la protección de datos personales. Este derecho fundamental a la protección de datos personales debe integrarse en los sistemas de compliance desde una doble faceta: de un lado, la protección de datos personales de los denunciantes y afectados por las denuncias en la gestión de los canales de denuncia internos y, de otro lado, en la creación de reglas en los códigos de buenas prácticas y riesgos para el interés público".

un plazo tres meses que podrá ampliarse a un máximo de los seis meses que determina la Ley[12](art.32.3 y 4) y sin perjuicio de lo previsto en el art.26 en relación con el libro-registro, si bien de acuerdo con los modos y plazos de conservación de los datos de carácter personal que hayan sido objeto de tratamiento. Lo anterior, no es óbice para una eventual conservación de los datos por aplicación, de otras normas que prevén distintas posibilidades de conservar determinada información, como las que se derivan del artículo 31bis.2 y artículo 31 quarter.1, letra d) del Código Penal, esto es los sistemas de *compliance*.

En esta línea, la Ley distingue de un lado, la información contenida en el sistema de información, de aquella otra del libro-registro del art.26, fijando que dicho libro-registro no será público y únicamente se podrá acceder a dicha información a petición razonada de la Autoridad judicial competente mediante auto, y en el marco de un procedimiento judicial y bajo la tutela de aquella, pudiéndose conservar durante los plazos en atención a la investigación y el tipo delictivo de que se trate. Sin embargo, para los datos personales de los informantes y terceros concernidos contenidos en los sistemas de información, se dispone que solo se conservarán durante el período que sea necesario y proporcionado a efectos de cumplir con esta ley, tal como se indica en los citados apartados 3 y 4 del artículo 32. En cualquier caso, si hubieran transcurrido tres meses desde la recepción de la comunicación sin que se hubieran iniciado las actuaciones de investigación, se procederá a la supresión de dichas informaciones, salvo que la finalidad fuera la de dejar evidencia del funcionamiento del sistema de información, pudiendo constar en el sistema las comunicaciones a las que no se hubiera dado curso, si bien de forma anonimizada.

Según el Informe 0060/2023[13] de la Agencia de Protección de Datos-AEPD- se permitiría compatibilizar la necesaria supresión de los datos personales en los sistemas internos de información, sometidos a un régimen de acceso más amplio una vez transcurridos los plazos que se recogen en el artículo 32 de la Ley, (limitados al tiempo imprescindible para decidir sobre la procedencia de iniciar una investigación), con un plazo máximo de tres meses, prorrogable por otros tres meses más de forma excepcional, transcurrido el cual deberán ser suprimidos o anonimizados, con la obligación de la entidad responsable del tratamiento de llevar el citado libro-registro, en el que se establece un plazo de conservación más amplio que puede alcanzar los diez años, y que tiene garantías específicas. En el citado Informe la autoridad de control, indica que el responsable del tratamiento en cuanto a los sistemas de *compliance,* y a los efectos "*de poder ejercer con todas las garantías los derechos previstos en el artículo 24 de la Constitución, en un hipotético procedimiento penal, en relación con lo dispuesto en el artículo 31 bis 2 y artículo 31 quarter 1. d) del Código Penal, pueda conservar en un espacio ajeno y distinto a los que se derivan de la Ley 2/2023 de 20 de febrero, aquella información que resulte necesaria a tal fin, precisamente para cumplir con las finalidades que justificarían dicho tratamiento con arreglo a otras leyes que también les obligan"*.

Al mismo tiempo, para proteger al informante y terceros afectados por las informaciones recibidas, si se acreditara que la información facilitada o parte de ella de los sistemas

[12]Informe 0060/2023 de la AEPD.

[13]De lo indicado hasta ahora se establece la existencia de dos espacios perfectamente diferenciados con un régimen distinto en términos cualitativos y cuantitativos. Por un lado, el Sistema Interno de Información, dónde los plazos de conservación de la información son como máximo de tres meses si no se han iniciado las actuaciones correspondientes, y, si se han iniciado las actuaciones, deberá estarse a los plazos del "procedimiento" que tramite el sujeto obligado y si bien no se indica expresamente en la ley, de sus preceptos se puede deducir, en principio, que es de seis meses en ciertos casos al indicar el artículo 9. 2 d) lo siguiente: 2. El procedimiento establecerá las previsiones necesarias para que el Sistema interno de información y los canales internos de información existentes cumplan con los requisitos establecidos en esta ley. En particular, el procedimiento responderá al contenido mínimo y principios siguientes: d) Determinación del 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 o, si no se remitió un acuse de recibo al informante, a tres meses a partir del vencimiento del plazo de siete días después de efectuarse la comunicación.

internos no es veraz, habrá de ser suprimida de forma inmediata, en cuanto se tuviera constancia de la ausencia de veracidad, excepto cuando dicha falta de veracidad pueda constituir un ilícito penal, en cuyo caso se conservará la información por el tiempo necesario durante el que se tramite el procedimiento judicial.

Con este mismo propósito de protección, los titulares de los datos personales en los sistemas internos de información deberán ser informados sobre sus datos personales en relación con las concretas denuncias en las que se vean involucrados (directa o indirectamente), por cuanto el art. 13 del RGPD, aplicable a los casos en los que los datos se obtengan directamente de los interesados, y el art. 14 del mismo texto, de aplicación a aquellos supuestos en los que estos no se obtengan de los interesados. El deber de información de la entidad obligada no se agota con la publicidad del canal de denuncias, tal y como únicamente exigen los artículos 24.1 de la LO 3/2018 y 32.5 de la Ley 2/2023, sino que exige igualmente dar dicho derecho respecto al tratamiento de los datos existentes en las informaciones.

Por su parte, resulta reseñable que el artículo 33[14] de la Ley 2/2023, fija como una medida de garantía, la preservación de dicha identidad tanto del informante como de los terceros afectados, garantizando no solo la confidencialidad de los datos correspondientes a los mismos, sino fijando que no será objeto del derecho de acceso a datos personales el dato de la identidad del denunciante, quedando limitada la posibilidad de dicha comunicación[15],y en consecuencia, la identidad del informante, que solo podrá ser comunicada, de acuerdo con su apartado 3[16], tratándose de la autoridad judicial, Ministerio fiscal o autoridad administrativa en el marco de una investigación, aunque cabe que el mismo pudiera haber optado por el anonimato.

En relación con la garantía del art. 33 de la Ley 2/2023, se preceptúa que quienes lleven a cabo una información o una revelación pública, se les habrá de informar de forma expresa, que su identidad será en todo caso reservada, que no se comunicará a las personas a las que se refieren los hechos relatados ni a terceros, siendo en este sentido taxativo el art.33.apart.1 de la Ley "*Quien presente una comunicación o lleve a cabo una revelación pública tiene derecho a que su identidad no sea revelada a terceras personas*".

No obstante, y a pesar de existir dicha regla general de la preservación de la identidad del denunciante, cabe la excepción a dicho *"pilar esencial "* en palabras de la Ley, cuando bien

---

[14] Los sistemas internos de información, los canales externos y quienes reciban revelaciones públicas no obtendrán datos que permitan la identificación del informante y deberán contar con medidas técnicas y organizativas adecuadas para preservar la identidad y garantizar la confidencialidad de los datos correspondientes a las personas afectadas y a cualquier tercero que se mencione en la información suministrada, especialmente la
identidad del informante en caso de que se hubiera identificado.
3. La identidad del informante solo podrá ser comunicada a la Autoridad judicial, al Ministerio Fiscal o a la autoridad administrativa competente en el marco de una investigación penal, disciplinaria o sancionadora.
Las revelaciones hechas en virtud de este apartado estarán sujetas a salvaguardas establecidas en la normativa aplicable. En particular, se trasladará al informante antes de revelar su identidad, salvo que dicha información pudiera comprometer la investigación o el procedimiento judicial. Cuando la autoridad competente lo comunique al informante, le remitirá un escrito explicando los motivos de la revelación de los datos confidenciales en cuestión.

[15] Ayala de la Torre J.M. y Bueno Sanchez, J.M La protección del informante en el Derecho español. Edit. Aranzadi. Madrid.2023, pag.157

[16] "a la Autoridad Judicial, al Ministerio fiscal o a la autoridad administrativa competente en el marco de una investigación penal, disciplinaria o sancionadora regulándose que las revelaciones que se realizaran en virtud de dicho apartado estarán sujetas a las salvaguardas establecidas en la normativa aplicable. En particular, se trasladará al informante antes de revelar su identidad, salvo que dicha información pudiera comprometer la investigación o el procedimiento judicial. Cuando la autoridad competente lo comunique al informante, le remitirá un escrito explicando los motivos de la revelación de los datos confidenciales en cuestión."

una norma nacional prevea revelarlo, o bien se solicite en el marco de un proceso judicial, con el fin de garantizar la tutela judicial efectiva y el derecho de defensa por parte del denunciado, ya que en este caso estarían en conflicto varios derechos fundamentales, con la necesaria ponderación entre los mismos y la aplicación del principio de proporcionalidad, tal como recuerda la Sentencia del Tribunal Constitucional 14/2003, de 28 de enero [17].

Dada la relevancia que la Ley otorga a la protección del informante, y por consiguiente, del principio de confidencialidad de acuerdo con el art. 32 de la Ley, se establecen unas limitaciones en cuanto a las personas que dentro de la entidad obligada puedan tener acceso a las informaciones, que queda muy restringida, dentro del ámbito de las competencias y funciones que correspondan, exclusivamente las personas de la organización en el citado precepto designadas[18].

5. LIMITACIONES DEL DERECHO DE DEFENSA ANTE LA PRESERVACIÒN DE LA IDENTIDAD.

Como ya hemos visto, la regulación de la Ley 2/2023 tiene como objetivo la prevención del fraude y la corrupción, a través de la implantación de sistemas internos y externos de información, evitando o detectando con ello prácticas que, en definitiva, implican importantes perjuicios para el interés público. No obstante, la Ley no supone una derogación de las restantes normas y obligaciones que responden a los mismos principios de fomento de la creación de una cultura ética y de cumplimiento, tanto del sector público, como del sector privado. En este sentido, la Ley 2/2023 no ha afectado a las normas relativas al proceso penal o que regulan el derecho de defensa en ese proceso y que afectan a las personas denunciadas, ya se trate de personas físicas o jurídicas, que cuentan cómo no puede ser de otra manera, con el Derecho Fundamental recogido en el art.24.2 de la Constitución española.

Conviene hacer referencia a que las denuncias a las que se refiere la Ley 2/2023 son totalmente distintas y compatibles con las denuncias judiciales, y como sostiene el Consejo del Poder Judicial en el Informe de 26 de mayo de 2022 al Anteproyecto de ley, incide en el hecho de la importancia de la finalidad de la Directiva y por tanto de la Ley 2/2023, que no es otro que "*alentar la denuncia interna, y proteger al informante, y en modo alguno penalizar a aquel que, precisamente para evitar represalias, acude a canales internos o*

[17] la STC 14/2003, de 28 de enero: "En otras palabras, de conformidad con una reiterada doctrina de este Tribunal, la constitucionalidad de cualquier medida restrictiva de derechos fundamentales viene determinada por la estricta observancia del principio de proporcionalidad. A los efectos que aquí importan basta con recordar que, para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple los tres requisitos o condiciones siguientes: si la medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto; SSTC 66/1995, de 8 de mayo [RTC 1995, 66] , F. 5; 55/1996, de 28 de marzo [RTC 1996, 55] , FF. 7, 8 y 9; 270/1996, de 16 de diciembre [RTC 1996, 270] , F. 4.e; 37/1998, de 17 de febrero [RTC 1998, 37] , F. 8; 186/2000, de 10 de julio [RTC 2000, 186] , F. 6)

[18] Art-32.a) El Responsable del Sistema y a quien lo gestione directamente. b) El responsable de recursos humanos o el órgano competente debidamente designado, solo cuando pudiera proceder la adopción de medidas disciplinarias contra un trabajador. En el caso de los empleados públicos, el órgano competente para la tramitación del mismo. c) El responsable de los servicios jurídicos de la entidad u organismo, si procediera la adopción de medidas legales en relación con los hechos relatados en la comunicación. d) Los encargados del tratamiento que eventualmente se designen. e) El delegado de protección de datos.2. Será lícito el tratamiento de los datos por otras personas, o incluso su comunicación a terceros, cuando resulte necesario para la adopción de medidas correctoras en la entidad ola tramitación de los procedimientos sancionadores o penales que, en su caso, procedan.

externos y evita denunciar ante la autoridad judicial, fiscal o policial,…..(…)" , determinando el art.2.2. de la Ley que "*Esta protección no excluirá la aplicación de las normas relativas al proceso penal incluyendo las diligencias de investigación*".

Singularmente, la Ley a pesar de proteger la identidad del informante, no ha afectado al Derecho Fundamental a la tutela judicial efectiva y Derecho de defensa, sino todo lo contrario, al determinar la aplicación de las normas relativas al proceso penal o que regulan el derecho de defensa en ese proceso y que afectan a las personas objeto de denuncia. Así lo indicaba expresamente el considerando 28 de la Directiva 2019/1937, al señalar que esta regulación "… *no debe afectar a las normas nacionales relativas al proceso penal, especialmente a las destinadas a proteger la integridad de las investigaciones y procedimientos o los derechos de defensa de las personas afectadas*". Criterio éste que se recoge igualmente en el artículo 3.3.d) de la Directiva, que fija que esa regulación no afecta a la aplicación del derecho de la Unión Europea o nacional relativo a las normas del enjuiciamiento criminal. Y el derecho de defensa de las personas afectadas expresamente se salva en el artículo 22.1 de la Directiva "*Medidas para la protección de las personas afectadas1. Los Estados miembros velarán, de conformidad con la Carta, por que las personas afectadas gocen plenamente de su derecho a la tutela judicial efectiva y a un juez imparcial, así como a la presunción de inocencia y al derecho de defensa, incluido el derecho a ser oídos y el derecho a acceder a su expediente*". Este reconocimiento y protección se recoge en la Ley 2/2023, que en su artículo 2.2, al definir el ámbito material de aplicación, dispone, como se ha indicado anteriormente, que "*Esta protección no excluirá la aplicación de las normas relativas al proceso penal, incluyendo las diligencias de investigación".*

Esta previsión normativa incluye las normas especiales que puedan existir como las de protección de testigos recogidas en la Ley Orgánica 19/1994, de 23 de diciembre, pero también se extiende a todas aquellas normas destinadas a proteger los derechos de defensa de las personas afectadas, en línea con lo señalado en la Directiva. Esta protección se reitera en el artículo 39.1, al definir las medidas para la protección de las personas afectadas "*Durante la tramitación del expediente las personas afectadas por la comunicación tendrán derecho a la presunción de inocencia, al derecho de defensa y al derecho de acceso al expediente en los términos regulados en esta ley, así como a la misma protección establecida para los informantes, preservándose su identidad y garantizándose la confidencialidad de los hechos y datos del procedimiento".*

Por otro lado, se ha de tener en cuenta, que una norma que no tiene el carácter de ley orgánica no puede interpretarse como una norma legal con habilitación suficiente para impedir o limitar el derecho de defensa del artículo 24.2 de la Constitución Española en sus distintas manifestaciones, esto es, para afectar al contenido esencial de un derecho fundamental de las partes afectadas en el proceso penal, con las garantías como a la no autoincriminación. Así lo ha reconocido el Tribunal Constitucional[19], destacando que la garantía de no auto incriminación es una especie de los derechos a no declarar contra sí mismo y a no confesarse culpable, que *"son garantías o derechos instrumentales del genérico derecho de defensa, al que prestan cobertura en su manifestación pasiva, esto es, la que se ejerce precisamente con la inactividad del sujeto sobre el que recae o puede recaer una imputación*". Estos derechos, según esas mismas sentencias, *"entroncan también con una de las manifestaciones del derecho a la presunción de inocencia, en virtud de la cual la carga de la prueba en el proceso penal corresponde a la acusación, sin que pueda hacerse recaer en el acusado la obligación de aportar elementos de prueba que supongan una autoincriminación*". También sobre el fundamento de esta garantía, el Tribunal Constitucional[20] ha recogido la doctrina del Tribunal Europeo de Derechos Humanos

[19] SSTC 197/1995, de 21 de diciembre, FJ 6; 161/1997, de 2 de octubre, FJ 5; 18/2005, de 1 de febrero, FJ 2; 142/2009, de 15 de junio, FJ 3, y con términos análogos en la STC 54/2015, de 16 de marzo, FJ 7).

[20] (SSTC 142/2009, FJ 3; 18/2015, FJ 2, y 54/2015, FJ 7)

(TEDH)[21], al indicar que "*el derecho a guardar silencio y el privilegio contra la autoincriminación son normas internacionales generalmente reconocidas que descansan en el núcleo de la noción de proceso justo garantizada en el art. 6.1 del Convenio. El derecho a no auto incriminarse, en particular, presupone que las autoridades logren probar su caso sin recurrir a pruebas obtenidas mediante métodos coercitivos o de presión en contra de la voluntad de la 'persona acusada"*.

En este sentido, la propia Directiva establece, para salvaguardar el derecho de defensa, una excepción al deber confidencialidad en su artículo 16.2, permitiendo que la identidad del denunciante u otra información sea revelada cuando exista una obligación legal necesaria y proporcionada en el contexto de una investigación o en el marco de un proceso judicial, para garantizar el derecho de defensa de la persona afectada, que deriva de la Directiva 2012/13/UE del Parlamento Europeo y del Consejo, de 22 de mayo de 2012, relativa al derecho a la información en los procesos penales, con su correspondiente reflejo en el artículo 33.3 de la Ley 2/2023 citado.

En consecuencia, esa compatibilidad debe resolverse por la vía de los artículos 2.2 y 40 de la Ley 2/2023, que permite entender que la regulación de estos sistemas internos de información no excluirá la aplicación de las normas relativas al proceso penal, incluyendo las diligencias de investigación. Normas relativas al proceso penal que incluyen el derecho a la defensa en los términos del artículo 24.2 de la CE. En efecto, en el caso de poder quedar afectado el derecho de tutela judicial efectiva y defensa del art.24.2 de la Constitución, quedaría limitado el derecho del informante y los terceros, por cuanto en caso de existir acciones u omisiones que puedan constituir infracciones del Derecho de la Unión Europea, o ser constitutivas de infracción penal o administrativa grave o muy grave, que se pusieren de manifiesto a través de este canal de información, se fija como obligación del responsable del sistema de información de la entidad de que se trate, la remisión con carácter inmediato al Ministerio Fiscal o la Fiscalía europea, y en caso de ser necesaria la revelación en el ámbito de una investigación penal, disciplinaria o sancionadora, se actuará conforme determina el art.33.3, mediante la comunicación que habrá de hacer al informante la autoridad competente de que se trate, siempre que no se comprometa la investigación o el procedimiento judicial.

Ahora bien, dicha necesidad de revelación aparece conectada como se ha indicado, en el concreto contexto de un procedimiento penal, al empleo de las alegaciones del denunciante como fuente de prueba y como testimonio de cargo en ese marco, como señala la STS de 23 de julio de 2022.

No obstante, el dato de la identidad del informante con respecto a la persona denunciada seguirá siendo confidencial, ya que la persona afectada no podrá recibir ninguna información sobre la identidad del informante, en la medida en que sea legalmente posible para garantizar sus derechos de tutela judicial y defensa, de acceso al expediente, de confidencialidad y reserva de identidad y la presunción de inocencia; en fin, de los mismos derechos de los que goza el informante, y a salvo de fijar la ponderación de los derechos fundamentales en conflicto, ya que ningún derecho fundamental es ilimitado, o absoluto.

En efecto, es el art.9.2.j de la Ley 2/2023, el que preceptúa la obligación por parte del responsable del sistema de "*Remisión de la información al Ministerio Fiscal con carácter inmediato cuando los hechos pudieran ser indiciariamente constitutivos de delito"* lo que podría implicar una declaración incriminatoria de la persona denunciada contraria a dicho principio, y en particular, en el caso de ser la denunciada la propia persona jurídica, responsable del sistema con la obligación de remisión, pues podría entenderse que con ello se vulnera el derecho a la no autoincriminación y a guardar silencio. En este punto, la

[21] (STEDH de 3 de mayo de 2001, caso J.B. c. Suiza, § 64; en el mismo sentido, SSTEDH de 8 de febrero de 1996, caso John Murray c. Reino Unido, § 45; de 17 de diciembre de 1996, caso Saunders c. Reino Unido, § 68; de 21 de diciembre de 2000, caso Heaney y McGuinness c. Irlanda, § 40; de 8 de abril de 2004, caso Weh c. Austria, § 39, y de 4 de octubre de 2005, caso Shannon c. Reino Unido, § 32).

doctrina ha puesto de relieve la dificultad teórica que representa la ausencia de una excepción expresa en la Ley que asegure la compatibilidad entre la obligación de denuncia indicada y su vinculación con la garantía del derecho fundamental de la persona jurídica afectada por la información, que podría salvarse, por la vía de la aplicación del art.2.2 y 40 de la Ley 2/2023.

6. LA GARANTÍA DEL ANONIMATO EN LAS DENUNCIAS

Otra de las medidas que la Ley 2/2023, permite es precisamente las denuncias anónimas con objeto de preservar su identidad del informante en el propio sistema, llevando su protección más allá de la confidencialidad, al impedir que ni el propio órgano encargado de la tramitación de las denuncias conozca la identidad del informante, cuestión ésta que podría llegar a comprometer incluso el derecho de defensa de la persona afectada por la denuncia, al enfrentarse a una investigación en la que desconoce la identidad de quien le acusa y la procedencia de la evidencia que contra él se aporta. En palabras de la propia Ley 2/2023 en su exposición de motivos, el fundamento "*ese canal interno de información al que hemos hecho referencia en párrafos anteriores debe garantizar, si queremos que salgan a la luz los comportamientos reprobables, la confidencialidad del informante, en todo caso, siendo aconsejable prever, además, el anonimato del mismo. No hay mejor forma de proteger al que informa que garantizando su anonimato.*"

Ha de recordarse que la denuncia anónima no es un elemento extraño ni en la normativa europea[22], ni la normativa vigente de carácter nacional, existiendo diversos ámbitos en los que se ha regulado la posibilidad de denuncias anónimas.[23]

No obstante, la Directiva *Whistleblowing*, por su parte, no impone a los Estados miembros la obligación de aceptar las denuncias anónimas, si bien, en caso de que así se establezca en el derecho nacional, las personas denunciantes cuyo anonimato llegara a desaparecer, deben gozar de la protección dispensada por la norma europea, tal y como determina claramente el considerando 34. Ante ello, el legislador nacional ha optado, por regular la posibilidad de informar de forma anónima tanto a través de los canales internos en su art.7.3, como de la Autoridad Independiente de Protección del Informante. En consecuencia,

[22] Directiva de Ejecución (UE) 2015/2392 de la Comisión, de 17 de diciembre de 2015, relativa al Reglamento (UE) núm. 596/2014 del Parlamento Europeo y del Consejo en lo que respecta a la comunicación de posibles infracciones o infracciones reales de dicho Reglamento a las autoridades competentes, donde se recogen las normas que especifican los procedimientos de denuncia del artículo 32.1 del Reglamento, incluyendo la posibilidad de que la denuncia se presente de forma anónima (artículo 5.1 a). Por otro lado, la Directiva (UE) 2015/849 del Parlamento Europeo y del Consejo, de 20 de mayo de 2015, relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales o la financiación del terrorismo, y por la que se modifica el Reglamento (UE) núm. 648/2012 del Parlamento Europeo y del Consejo, recoge dos normas en su artículo 61: (i) la confidencialidad cuando se trata de la denuncia a las autoridades competentes (artículo 61.2 e) y (ii) el anonimato cuando se comunican infracciones a nivel interno en una entidad (artículo 61.3).

[23] Ley 10/2010, modificada por Real Decreto Ley 11/2018, se introdujo en la ley de prevención del blanqueo de capitales y de la financiación del terrorismo, el actual art. 26 bis en el que se regulan los procedimientos internos de comunicación de potenciales incumplimientos (canales de denuncias interna) para que sus empleados, directivos o agentes puedan comunicar, incluso anónimamente, información relevante sobre posibles incumplimientos de esta ley, su normativa de desarrollo o las políticas y procedimientos implantados para darles cumplimiento, cometidos en el seno del sujeto obligado. Y en la LO 12/2007, de régimen disciplinario de la Guardia Civil también se contemplaba la posibilidad de denuncias anónimas en las informaciones sobre actos u omisiones en una organización(denuncia interna) o a una autoridad externa(denuncia externa) como a las personas que ponen dicha información a disposición del público, por ejemplo directamente a través de plataformas web o de redes sociales, o a través de medios de comunicación, cargos electos, organizaciones de la sociedad civil, sindicatos u organizaciones profesionales y empresariales.

la regla general ha sido la regulación de las informaciones anónimas y proteger a la persona que las comunica.

A pesar de que el artículo 24.1[24] de la LO 3/2018, regulaba ya la creación y mantenimiento de sistemas de información internos de forma anónima, la nueva Ley 2/2023 ha incluido una serie de previsiones y reglas necesarias respecto a los datos personales, no solo en los casos de los canales internos de información en entidades privadas y públicas, sino a través de los canales externos y contemplando los supuestos de revelación pública. Sobre el anonimato ya se había pronunciado el Grupo de trabajo del art.29 en su Dictamen 1/2006[25] , lo que también se recoge en el preámbulo de la Ley 2/2023 en el apartado III, en el que se mantiene "*desde las instituciones de la Unión Europea se ha apostado sin ambages por la posibilidad de la aceptación y seguimiento de las denuncias anónimas. A tales efectos, se puede acceder a una herramienta de "denuncia anónima" de irregularidades para ayudar a la Comisión Europea a descubrir cárteles y otras infracciones antimonopolio y sobre tales prácticas anticompetitivas prohibidas por la normativa de competencia de la Unión Europea, que causan daños considerables a la economía europea*."

7. LAS GARANTÍAS EN LOS CASOS DE REVELACIÓN PÚBLICA

Por su parte, quien lleve a cabo una revelación pública tiene derecho a que su identidad no sea revelada a terceras personas, existiendo una limitación clara al derecho de acceso dispuesto en la Ley, sin perjuicio de lo previsto en el artículo 33 de la Ley 2/2023. En este sentido, se pronuncia el Consejo de Estado en su Informe de 26 de mayo de 2022 sobre el anteproyecto de Ley. A los informantes o a quienes lleven a cabo una revelación pública, el tratamiento de sus datos únicamente se efectuará bajo la presunción de lo dispuesto en los artículos 6.1.e) del RGPD y 11 de la LO 7/2021, a los que se informará de forma expresa que su identidad será en todo caso reservada y que no se comunicará a las personas a las que se refieren los hechos relatados ni a terceros[26].

Precisamente una de las cuestiones más complejas de la regulación es la protección del informante y sus derechos cuando nos encontramos ante supuestos de revelación pública. Por tanto, estas garantías de protección del informante cobran mayor relevancia en estos casos, pero solo si se cumplen alguna de las condiciones enumeradas en el propio texto, con un especial reconocimiento a los supuestos de protección relacionados con los derechos a la libertad de expresión y de información y pluralismo de los medios de comunicación[27] que, en nuestro Derecho se reconocen como Fundamentales en el art. 20.1 CE, respecto de las personas que ponen dicha información a disposición del público, por ejemplo como consecuencia del deber de diligencia del informador[28] a quien se debe exigir que lo que trasmita como hechos denunciados hayan sido previamente contrastados[29].

El art.15 de la Directiva, determina respecto a la revelación pública, que "*La persona que haga una revelación pública podrá acogerse a protección en virtud de la presente Directiva*

[25] Relativo a la "aplicación de las normas sobre protección de datos de la UE a los sistemas internos de denuncia de irregularidades en los ámbitos de la contabilidad, controles y cuestiones de auditoría, lucha contra la corrupción y delitos financieros y bancarios", establecía como regla general que el denunciante debía identificarse, pero también existía la posibilidad de recibir y tramitar denuncias anónimas en determinadas circunstancias.

[26] Art.31 de la L2/2023.

[27] STC 30/2022, de 7 de marzo " la libertad reconocida en el art.20.1d) CE, en cuanto transmisión de manera veraz de hechos noticiables, de interés general y relevancia pública, no se erige únicamente en derecho propio del titular sino en una pieza esencial en la configuración del Estado democrático, garantizando la formación de una opinión publica libre y la realización del pluralismo como principio básico de convivencia".

[28] STC 6/1988, de 21 de enero.

[29] Ayala de la Torre J.M. y Bueno Sanchez, J.M: La protección del informante en el Derecho español. Edit. Aranzadi. Madrid.2023, pag.150

si se cumple alguna de las condiciones siguientes: a) la persona había denunciado primero por canales internos y externos, o directamente por canales externos de conformidad con los capítulos II y III, sin que se hayan tomado medidas apropiadas al respecto en el plazo establecido en el artículo 9, apartado 1, letra f), o en el artículo 11, apartado 2, letra d), o b) la persona tiene motivos razonables para pensar que: i) la infracción puede constituir un peligro inminente o manifiesto para el interés público, como, por ejemplo, cuando se da una situación de emergencia o existe un riesgo de daños irreversibles, o ii) en caso de denuncia externa, existe un riesgo de represalias o hay pocas probabilidades de que se dé un tratamiento efectivo a la infracción debido a las circunstancias particulares del caso, como que puedan ocultarse o destruirse las pruebas o que una autoridad esté en connivencia con el autor de la infracción o implicada en la infracción. Por su parte, el Título V de la Ley se ocupa de la revelación pública, contando los informantes que utilicen tanto los canales internos de información, como el canal externo que se crea ante la A.A.I., con un régimen específico frente a las represalias.[30] En el artículo 27 de la Ley 2/2023, se parte de un concepto de revelación pública como la puesta a disposición del público de información sobre las acciones u omisiones en los términos previstos en la Ley, y se distingue cuando una persona accede directamente a la prensa y denuncia allí, encontrándose en dicho supuesto protegido en el marco del ejercicio de la libertad de expresión y de información[31], siendo la información que se protege la que se trasmita de forma veraz.

En efecto, nuestro legislador nacional incorpora a la Ley la revelación pública en los artículos 27 y 28 de la Ley, distinguiendo si la revelación pública se hace por medios distintos a la prensa, aplicándose el art.28.1 de la Ley, exigiendo como una de las dos condiciones para ser tenida en cuenta: o bien que se haya realizado la comunicación primero por los canales internos o externos o directamente por los canales externos y no se hayan tomado medidas apropiadas; o que el informante tenga motivos razonables[32] para pensar que o bien la infracción constituye un peligro inminente para el interés público, o bien en caso de comunicación a través de canal externo, que exista un riesgo de represalias o haya pocas probabilidades de que se dé un tratamiento efectivo debido a las circunstancias del caso, tales como la ocultación o destrucción de pruebas, la connivencia de una autoridad con el autor de la infracción o que ésta esté implicada en la infracción.

En este sentido, la doctrina constitucional contiene ya desde hace tiempo precedentes claramente favorables para aquellos trabajadores que acuden a la revelación pública[33]. Si

---

[30] La propia exposición de motivos de la Ley indica "que la protección a quien realiza una revelación pública, con condiciones, se asienta, entre otras causas, en las garantías y protección que ofrece la opinión pública en su conjunto amparando a quien muestra una actitud cívica a la hora de advertir ante posibles infracciones penales o administrativas graves o muy graves o vulneraciones del ordenamiento jurídico que dañan el interés general, así como en la protección de las fuentes que mantienen los periodistas."

[31] la STC 6/1988, de 21 de enero, "especifico deber de diligencia del informador, al que se le debe exigir que lo que trasmita como hechos haya sido previamente contrastado, y ello sin perjuicio de la problemática que plantea el de la veracidad de las fuentes indeterminadas y su remisión a las mismas, siendo insuficiente a la hora de entender satisfecho el requisito de la veracidad de la información, que opera como requisito del derecho de información".

[33] STC 6/1998, de 21 de enero, que declaró la nulidad del despido disciplinario de un trabajador destinado en el gabinete de prensa del Ministerio de Justicia que se había justificado en transgresión de la buena fe contractual por haber aquel denunciado públicamente que, desde la llegada al poder del PSOE, se filtraban noticias de manera privilegiada a la Editorial Prisa (en el mismo sentido, la Sentencia de 12 de abril de 1999), aunque el Tribunal Constitucional ha matizado esta doctrina favorable, siendo claro ejemplo de ello la Sentencia de 30 de junio de 2003.

la revelación se hace a través de la prensa y denuncia allí, se aplica el art.28.2.[34] quedando el informante protegido por los derechos que otorga la Ley, siempre que se encuentre dentro de los límites normales del ejercicio de la libertad de expresión y de información. En los artículos 35 a 40 de la citada Ley se fijan las medidas de protección de las personas afectadas, de prohibición de represalias, en la misma línea que hace la Directiva en su art. 19, donde se relacionan una serie de supuestos enunciativos como posibles actos considerados de represalia. La protección de los informantes frente a las represalias se fija a un período de 2 años, período que podría ser extendido en determinadas situaciones excepcionales[35].

Por último, reseñar que en la Directiva en sus artículos 20 y 21 fija los medios de apoyo contra el informante ante los actos de represalia, obligando a los estados miembros en el sentido que "*adoptarán las medidas necesarias para garantizar que las personas a que se refiere el artículo 4 estén protegidas frente a represalias. Dichas medidas incluirán, en particular, las que figuran en los apartados 2 a 8 del presente artículo*". En la Ley nacional, se regula la necesidad de concurrencia de una serie de condiciones que son las que determinarán la aplicación de las medidas de apoyo[36] previstas en el art.37 y los programas de clemencia como los denomina la Doctrina en su art.40, bajo la rúbrica de "*supuestos de exención y atenuación de la sanción"*, que admite que la persona informante que haya participado en la comisión de la infracción no sea sancionada con ello, si revela información importante que lleve al conocimiento del hecho delictivo, cuando en el mismo hubieran participado personas varias. No obstante, para dicha exención se requiere igualmente determinados requisitos, siendo el órgano competente el habilitado para en los casos que proceda atenuar la sanción

8. BIBLIOGRAFÍA

Ayala de la Torre, J.M. "Sombras en la aplicación de la Directiva *Whistleblower* y su transposición al derecho interno español". Revista de abogados del Estado, núm.58(2022)

---

[34] Art.28.2 "las condiciones para acogerse a la protección previstas en el apartado anterior no serán exigibles cuando la persona haya revelado información directamente a la prensa con arreglo al ejercicio de la libertad de expresión y de información veraz previstas constitucionalmente y en su legislación de desarrollo".

[35] No obstante, sobre los términos de la posibilidad de protección con anterioridad a la entrada en vigor de la Ley 2/2023, y su disposición sexta, hemos de citar la reciente Sentencia 1065/2023, de 20 de julio, Sección Tercera de la Sala de lo Contencioso del Supremo en su sentencia 1065/2023 de 20 de julio, señala que no puede revisar en casación la interpretación del derecho autonómico efectuada por el TSJCV de la ley valenciana que regula de la Agencia Valenciana Antifraude contra una sentencia que anuló su acuerdo de conceder el estatuto de denunciante protegido a un funcionario del Ayuntamiento de Los Montesinos (Alicante) que denunció ante un Juzgado de Torrevieja hechos presuntamente corruptos, teniendo en cuenta que la resolución sobre la protección del informante se efectuó 20 días antes de la entrada en vigor de la Directiva 2019/1937.

[36] a) Información y asesoramiento completos e independientes, que sean fácilmente accesibles para el público y gratuitos, sobre los procedimientos y recursos disponibles, protección frente a represalias y derechos de la persona afectada.

b) Asistencia efectiva por parte de las autoridades competentes ante cualquier autoridad pertinente implicada en su protección frente a represalias, incluida la certificación de que pueden acogerse a protección al amparo de la presente ley.

c) Asistencia jurídica en los procesos penales y en los procesos civiles transfronterizos de conformidad con la normativa comunitaria.

d) Apoyo financiero y psicológico, de forma excepcional, si así lo decidiese la Autoridad Independiente de Protección del Informante, A.A.I. tras la valoración de las circunstancias derivadas de la presentación de la comunicación.

2. Todo ello, con independencia de la asistencia que pudiera corresponder al amparo de la Ley 1/1996, de 10 de enero, de asistencia jurídica gratuita, para la representación y defensa en procedimientos judiciales derivados de la presentación de la comunicación o revelación pública.

Ayala de la Torre, JM y Bueno Sanchez, J.M, La protección del informante en el Derecho español, Tras la Directiva *Whistleblower* y la Ley 2/2023, de 20 de febrero. Edit. Aranzadi. Navarra 2023.

Calvo Verger, J. "Estructura, contenido y alcance de la Directiva (UE) 2019/1937, del Parlamento 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". Revista Aranzadi Unión Europea, num.5/2020, parte Doctrina, Editorial ARANZADI, S.A.U., Cizur Menor. (2020)

Campos Acuña, C; "Aproximación a la ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción: una visión aplicativa en el sector público". Revista Digital Centro de Estudios Municipales y Cooperación Internacional. CEMCI 2023 y Campos Acuña, C; "las 15 claves del Sistema Interno de información (*Whistleblower)*". Diario La Ley Nº 10234, 22 de febrero

Fernández Ramos, S.: "Ley 2/2023, de 20 de febrero, de protección al informante: ámbito material de aplicación".Número 63 de la Revista General de Derecho Administrativo (Iustel, mayo 2023)

Obispo Triana, C, Nuevas obligaciones y derechos con la ley de protección del informante y lucha contra la corrupción. Aranzadi digital num.1/2023, parte estudios y comentarios, Editorial Aranzadi. S.A.U.(2020)

Rebollo Delgado, L Inteligencia artificial y derechos fundamentales. Edit. Dykinson, (Madrid 2023)

Saez Hidalgo, I: "El ámbito objetivo de aplicación de la Ley 2/2023: ¿Qué comunicaciones pueden amparar el derecho a protección frente a las represalias?". Diario La Ley, Nº 10274, abril de 2023.

Vazquez de Castro, E; "La doble faceta de la protección de datos personales en los sistemas de *compliance*". Revista Aranzadi de Derecho y Nuevas Tecnologías, numero 59 (2022)