**Canal de denuncias.**

**Contexto regulatorio.**

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**, viene a transponer al ordenamiento jurídico español la Directiva 2019/1937 del Parlamento Europeo y del Consejo, de 23 de octubre de 2019, relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión.

En la ***Directiva Whistleblowing*** se emplea el término «denunciante» mientras que la Ley 2/2023 española ha optado por la denominación «informante».

La Ley 2/2023 explica y aclara en su preámbulo que su finalidad es la de proteger, frente a posibles represalias, 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, (tanto en sector privado como en sector público).

A tal efecto, la Ley 2/2023 impone a cualquier entidad u organismo obligado por esta ley a disponer de un cauce preferente para informar sobre las acciones e infracciones referidas en la propia ley, denominado en la citada ley como "**sistema interno de Información**" y obliga también a cada entidad u organismo a contar con una política o estrategia que enuncie los principios generales en materia del sistema interno de información y defensa del Informante. Esta política debe ser debidamente publicitada en el seno de cada organización.



La finalidad del "canal" es doble, por un lado, hacer posible la comunicación por parte de personas que, en un contexto laboral o profesional, a las que se refiere el artículo 3 de la Ley, detecten infracciones penales o administrativas graves o muy graves previstas en el artículo 2 de la Ley; y por otro, que esas personas estén protegidas frente a posibles represalias.

**Sujetos obligados.**

La Ley 2/2023, de 20 de febrero, que traspone la conocida como **Directiva whistleblowing** (D2019/1937), establece la obligación de las empresas con más de 50 trabajadores y de todas las entidades públicas de disponer de un sistema interno de información mediante el que los trabajadores puedan informar sobre vulneraciones del ordenamiento jurídico en el marco de una relación profesional.

Así, conforme establece el artículo 10 están obligadas a disponer de un canal de denuncias interno las siguientes entidades del sector privado:

**1)** Empresas privadas con 50 o más trabajadores, (aunque se permite que las que cuenten con menos de 250 trabajadores pueden compartir medios y recursos para la gestión de las informaciones que reciban).

**2)** Empresas privadas entren en el ámbito de aplicación de los actos de la UE en materia de servicios, productos y mercados financieros, prevención del blanqueo de capitales o de la financiación del terrorismo, seguridad del transporte y protección del medio ambiente.

Llegados a este punto, en relación con el ámbito regulatorio del blanqueo, encontraríamos a las asesorías contables y fiscales, y los auditores de cuentas, como

sujetos obligados por la Ley de Prevención del Blanqueo de Capitales (art. 2.1. letra m) LPBC), y los abogados y otros profesionales (en la medida que realicen las actividades previstas por el art. 2.1 letra ñ) LPBC) deberán cumplir con una nueva normativa que les obliga a establecer un canal de denuncias, independientemente del número de trabajadores que tengan, salvo la exclusión reglamentaria que veremos a continuación. Todos los sujetos obligados deben cumplir 3 tipos de obligaciones:

De diligencia debida.
Obligaciones de información (al SEPBLAC).
Obligaciones de control interno.

Y en relación con el canal de denuncias en materia de blanqueo de capitales: desde el 4 de septiembre de 2018, todos los sujetos obligados, salvo que reglamentariamente sean exceptuados, deben de contar con lo que la Ley 10/10 llama “Procedimientos internos de comunicación de potenciales incumplimientos” (art. 26 bis Ley 10/10, introducido por RD-ley 11/18), es decir, canales de denuncias.

Como consecuencia de lo expuesto, estos canales de denuncias se ubican dentro de las obligaciones de control interno, y como el art. 26 bis L 10/10 se remite a excepciones reglamentarias, hay que acudir a la normativa reglamentaria.

Pues bien, puede entenderse que esta exclusión se encuentra recogida en el Reglamento de la Ley 10/10, aprobado por RD 304/14, cuando en su art. 31 sobre procedimientos de control interno, en su apartado 1 dice lo siguiente:

*“Los sujetos obligados aprobarán por escrito y aplicarán políticas y procedimientos adecuados de prevención del blanqueo de capitales y de la financiación del terrorismo. Los corredores de seguros y los sujetos obligados comprendidos en los apartados i) a u), ambos inclusive, del artículo 2.1 de la Ley 10/2010, de 28 de abril, que, con inclusión de los agentes, ocupen a* ***menos de 10 personas*** *y cuyo volumen de negocios anual o cuyo balance general anual* ***no supere los 2 millones*** *de euros, quedan exceptuados de las obligaciones referidas en este artículo y en los artículos 32, 33, 35, 38 y 39. Estas excepciones no serán aplicables a los sujetos obligados integrados en un grupo empresarial que supere dichas cifras”.*

En relación con los "colectivos profesionales", se puede llegar a la conclusión de que la obligación de contar con un canal de denuncias afecta a auditores, contables externos y asesores fiscales [art. 2.1.m) Ley 10/10], asi como a los “abogados, procuradores u otros profesionales independientes” [artículo 2.1.ñ Ley 10/10], SOLO cuando empleen a 10 o más personas o tengan un balance general anual igual o superior a 2 millones de euros (por aplicación de la excepción del art. 31.1 párr. 2º del RD 304/14). No aplica si forman parte de un grupo que supere esas cifras.

Es decir, si se reúnen las características descritas, entendemos que aplica la **excepción** para no implantar un sistema de información interno en línea con lo estipulado en la ley 2/2023.

**3)** Partidos políticos, los sindicatos, organizaciones empresariales y sus fundaciones siempre que reciban o gestionen fondos públicos.

**4)** Y por otro lado todas las entidades que integran el sector público (artículo 13 y ss). Los municipios de menos de 10.000 habitantes, podrán compartir el Sistema interno de información entre sí o con cualesquiera otras Administraciones públicas que se ubiquen dentro de la CCAA. Asimismo, las entidades con personalidad jurídica propia vinculadas o dependientes de órganos de las Administraciones territoriales, y que cuenten con

menos de 50 trabajadores, podrán compartir con la Administración de adscripción el Sistema interno de información.

**Relación con el ámbito del "compliance penal".**

Sin perjuicio de lo anterior, las personas jurídicas del sector privado que no estén sujetas a la obligación impuesta por la Ley podrán establecer (voluntariamente) su propio sistema interno de información, que deberá cumplir, en todo caso, los requisitos previstos en esta ley.

Esto aplicaría por ejemplo a cualquier empresa que decida adoptar la norma ISO 37301 sobre sistemas de gestión de compliance, y del mismo modo a las empresas que tengan un plan voluntario de compliance penal o programa de prevención de delitos, y también a los sujetos obligados por la regulación de blanqueo, y a las empresas que implementan un plan de igualdad.

Al hablar del modelo de prevención y control nos referimos al modelo de organización y gestión previsto en la reforma del Código Penal de 2015.

En el ordenamiento jurídico español, desde el año 2010, pero sobre todo a partir de la reforma del Código Penal, que entró en vigor el 1 de julio de 2015, las personas jurídicas pueden ser consideradas sujetos activos del delito. Antes de las reformas, el principio que seguía el Derecho español era el de negar que estas entidades pudieran delinquir.

La responsabilidad penal de las personas jurídicas tiene una peculiar estructura, pues exige la concurrencia de una serie de requisitos. En primer lugar, es precisa la comisión previa de un delito de los establecidos en el artículo 31 bis —una lista cerrada de más de 26— por una persona física, sea un administrador o representante legal, directivo o empleado.



Luego, es necesario que la falta se haya cometido en beneficio directo o indirecto de la sociedad que, sin embargo, quedará exenta de responsabilidad si acredita tener implantados modelos de gestión, vigilancia y supervisión eficaces, orientados a la prevención de delitos.

La Fiscalía General del Estado ha destacado que estos programas no pueden tener como único objetivo evitar la sanción penal de la compañía, sino que su principal finalidad debe ser promover una verdadera cultura ética empresarial.

"*La empresa debe contar con un modelo para cumplir con la legalidad en general y, por supuesto, con la legalidad penal, pero no solo con ella", dice la Circular 1/2016 de esa Fiscalía General. También deben ser claros, precisos, eficaces, conocidos por los destinatarios y estar redactados "por escrito". No bastará con la mera existencia de un programa, sino que deberá acreditarse su adecuación para prevenir el concreto delito que se ha cometido, debiendo realizarse un juicio de idoneidad entre el contenido del programa y la infracción cometida. Por ello, "deben estar perfectamente adaptados a la compañía y a sus concretos riesgos*".

Estos programas de cumplimiento son una herramienta esencial para las empresas para defenderse de la imputación de delitos. Es más, el Tribunal Supremo ha establecido que la prueba de la "idoneidad" de los programas corresponde a la acusación. A la vez, ha quedado sentado que las personas jurídicas gozan de los mismos derechos que las personas físicas, en el proceso penal.

**Protección de datos.**

Se ha de destacar que se permite la comunicación anónima. Cuando se traslade una comunicación en el marco del sistema interno de información, que entre dentro del ámbito de aplicación de la ley, se aplicará la regla específica contenida en esta ley en cuanto a la posibilidad de presentación y tramitación de comunicaciones anónimas. La Directiva establece como principio el deber general de mantener al informante en el anonimato. Ahora bien, este pilar esencial de la norma europea se exceptúa cuando, bien una norma nacional prevé revelarlo, o bien se solicita en el marco de un proceso judicial, lo que ocurre en muchas ocasiones, argumentando el juzgador la necesidad de conocer la identidad de quien denunció, para garantizar el derecho de defensa del denunciado (ver considerando 34 y art. 6.2).

Así pues, la información puede comunicarse a la organización de forma anónima. En otro caso, se reservará la identidad del informante de forma confidencial y quedará limitada al conocimiento del órgano de cumplimiento encargado específicamente del canal.

Es decir, en la regulación española coexisten las dos posibilidades, siendo asi que el canal de denuncias anónimo permite las denuncias sin ningún tipo de identificación, mientras que el confidencial debe garantizar la preservación de los datos identificativos del denunciante.

Además, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, contempla (art. 24) la creación y mantenimiento de sistemas de información a través de los cuales pueda ponerse en conocimiento de una entidad de Derecho privado, incluso anónimamente, la comisión, en el seno de la misma o en la actuación de terceros que contratasen con ella, de actos o conductas que pudieran resultar contrarios a la normativa general o sectorial que le fuera aplicable.

Como antecedentes, el Grupo de Trabajo del art.29 -actual CEPD- (Dictamen 1/2006). Este órgano se postula hacia canales de denuncia abiertos, es decir, de manera identificada, fundamentándolo hasta en seis razones diferentes, pero a pesar de su preferencia, no rechaza de forma categórica la posibilidad de que se puedan dar denuncias de forma anónima.

Y por su parte la Agencia Española de Protección de Datos (Informe 128/2007) aconsejaba evitar la existencia de denuncias anónimas, garantizándose así la exactitud e integridad de la información contenida en dichos sistemas. Actualmente, este informe ha quedado superado por LOPD art.24, que sí permite la denuncia anónima.

Hasta ahora el artículo 24 de la citada ley orgánica regulaba la creación y mantenimiento de sistemas de información internos. El contenido de dicho precepto se ha incorporado a la Ley 2/2023, pero era necesario completar las previsiones hasta ahora incluidas en la ley orgánica al objeto de extenderlas también a los tratamientos de datos que se lleven a cabo en los canales de comunicación externos y en los supuestos de revelación pública.

Asimismo, y de acuerdo con lo que establece el artículo 6 del Reglamento general de protección de datos, procede indicar los títulos que hacen lícito el tratamiento de datos personales.

Los tratamientos se entenderán necesarios para el cumplimiento de una obligación legal cuando deban llevarse a cabo en los supuestos en que sea obligatorio disponer de un sistema interno de información y en los casos de canales de comunicación externos, mientras que se presumirán válidos al amparo de lo que establece el artículo 6.1.e) del

Reglamento general de protección de datos cuando aquel sistema no sea obligatorio o el tratamiento se lleve a cabo en el ámbito de la revelación pública que regula el título V.

Se indica asimismo que en caso de que la persona investigada ejerza el derecho de oposición al tratamiento de sus datos personales se entiende que existen motivos legítimos imperiosos que legitiman continuar con dicho tratamiento, tal como permite el artículo 21.1 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.
Salvo mejor opinión

**BOE**: 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.