TRABAJO FINAL DE GRADO

Doble grado de Administración y Dirección de Empresas y Derecho

Título: Los efectos de la Ley 2/2023 en las empresas. Nuevas obligaciones para las organizaciones.

Autoría: Marta Pérez Insúa

Tutoría: Fernando Barbancho Tovillas

Departamento: Derecho Privado

Curso académico: 2022-2023

UNIVERSITAT DE BARCELONA

Facultat d'Economia i Empresa

RESUMEN EJECUTIVO

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 es la transposición de la Directiva 2019/1937. La Ley tiene por objeto la protección de las personas informantes sobre infracciones del Derecho de la Unión Europea, así como otras acciones u omisiones que puedan ser constitutivas de infracción penal o administrativa grave o muy grave.
La norma implica un conjunto de obligaciones para las organizaciones, ya sean públicas o privadas, entre las que destaca la obligación de implantar un Sistema interno de información, que garantice la confidencialidad de la identidad del informante, junto con la no existencia de represalias, así como la correcta gestión de la información.

Palabras clave*: informante, denuncia, protección, represalias, canal,* compliance

ABSTRACT

Directive 2019/1937 has been transposed by Law 2/2023 of 20 February on the protection of persons who report infringements of the law and the fight against corruption. The purpose of the law is the protection of persons who report infringements of European Union law, as well as other acts or omissions which may constitute a serious or very serious criminal or administrative offence.
The regulation imposes a number of obligations on organisations, whether public or private, including the obligation to implement an internal information system that guarantees the confidentiality of the whistleblower's identity, the absence of retaliation and the correct management of information.

Keywords: *whistleblower, report, protection, reprisals, channel, compliance*

ÍNDICE

I. INTRODUCCIÓN

En los últimos años y, fruto principalmente de la introducción en 2010 de la responsabilidad penal de las empresas en el Código Penal Español, las empresas han empezado a dotarse de instrumentos de cumplimiento normativo o *compliance*.

Las empresas tienen actualmente, además, múltiples obligaciones formales "sobrevenidas" por ejemplo en materia de privacidad, de igualdad, de prevención del acoso en el trabajo, etc.

La Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción, en adelante Ley 2/2023, es una nueva fuente de obligaciones para las empresas españolas.

Los efectos de la Ley 2/2023, en las empresas y sus nuevas obligaciones es un tema sumamente relevante en el mundo empresarial actual. Esta ley ha establecido una serie obligaciones, medidas y requisitos que deben cumplir las organizaciones, y su incumplimiento puede tener importantes consecuencias en términos de responsabilidad social, reputación empresarial y en términos de posibles sanciones.

La motivación para llevar a cabo un trabajo de investigación en este ámbito es múltiple. Por un lado, existe en la sociedad un interés creciente en el cumplimiento de las normas y en la prevención de la corrupción, tanto por parte de los consumidores como de los inversores y otros agentes empresariales. Además, el análisis de los efectos de la Ley 2/2023, puede proporcionar una visión clara de las implicaciones y desafíos que deben enfrentar las empresas a la hora de adaptarse a las nuevas exigencias regulatorias.

Con este análisis de la norma se pretende entender la motivación y la necesidad de la nueva norma; analizar la norma jurídicamente, así como los efectos que tendrán tanto la entrada en vigor de la norma como el uso de la misma a largo plazo, a través de un análisis de las opiniones de los diferentes sectores profesionales a los que afectará. Para ello, se ha realizado un estudio exhaustivo de la materia a través de la propia norma, artículos, exposiciones y varias entrevistas con profesionales ligados al cumplimento normativo o *compliance* que trabajan con esta norma diariamente.

El trabajo se divide en una primera parte más teórica, analizando los antecedentes que llevan a la *Directiva (UE) 2019/1937 del Parlamento Europeo y del Consejo de 23 de octubre de 2019 relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión*, así como la propia Directiva. Sigue con la descripción del proceso de transposición, tardía, que hizo España, el análisis teórico de la nueva Ley 2/2023 y finalmente, un análisis de las diferencias entre ambas. La segunda parte del trabajo, más práctica, es donde se estudian casos reales de aplicación de la norma y las situaciones con las que se encuentran los profesionales que trabajan con ella. Finalmente se

ponen de relieve algunas cuestiones conflictivas que genera la aplicación de la norma, en, por ejemplo, el encaje de otras obligaciones formales de las empresas que pueden suponer una excesiva burocratización de la gestión.

Finalmente, agradecer a mi madre el apoyo, la orientación y el acompañamiento en el mundo del cumplimiento normativo de las empresas, así como a lo largo de mi experiencia académica. También agradecer a todos los entrevistados que han contribuido desinteresadamente en el éxito de este trabajo: Ana María Regada, compliance officer de Danone, Josep Jover, abogado, presidente de Aspertic, Lourdes Parramon i Bregolat, cap de l'àrea de relacions institucionals de l'Oficina Antifrau de Catalunya y Isabel Vizcaino, abogada y Presidenta de la Sección de Compliance del Colegio de la Abogacía de Barcelona.

II. ANTECEDENTES LEGALES

2.1 Origen y evolución del *Whistleblowing*

Un *Whistleblower*, según el diccionario inglés de Cambridge, es una persona que informa a alguien con autoridad sobre algo ilegal que está ocurriendo, especialmente en un departamento gubernamental o en una empresa. Es lo que en España se conoce como "chivato" y tradicionalmente, ser un chivato está mal visto.

La Convención de Naciones Unidas contra la corrupción del 31 de octubre de 2003, ratificada por España el 9 de junio de 2006 determina que los entes públicos deben establecer mecanismos y sistemas que faciliten que los servidores públicos denuncien cualquier acto de corrupción ante las autoridades competentes, cuando tengan conocimiento de ellos en el ejercicio de sus funciones. También fija la necesidad de proteger a las personas que, en cumplimiento de su deber ciudadano, denuncien casos de fraude o corrupción, asegurando su indemnidad. Además prevé la necesidad de ofrecer formación y sensibilización, capaces de crear una cultura de rechazo de toda conducta que propicie la corrupción. Concretamente, el artículo 5 de la Convención, prevé la obligación de formular y aplicar políticas contra la corrupción que promuevan la participación de la sociedad y reflejen los principios del imperio de la ley, la adecuada gestión de los asuntos y bienes públicos, la integridad, la transparencia y la obligación de rendir cuentas.

En 2019 se publicó la Directiva 2019/1937, relativa a la protección de las personas que informen sobre infracciones de derecho de la Unión Europea, conocida como la Directiva *Whistleblowing*, que tiene como objetivo principal asegurar que las personas trabajadoras tengan a su alcance un instrumento que les permita revelar posibles infracciones o irregularidades que puedan estar sucediendo en la empresa, garantizando la confidencialidad del denunciante. Pretenden así que se creen entornos más éticos en las empresas u organizaciones públicas.

Los legisladores a nivel europeo se dieron cuenta de que a menudo, son aquellos que trabajan en las organizaciones públicas o privadas o tienen contacto directo con ellas las que, en el transcurso diario de su actividad, son las primeras en conocer las amenazas o perjuicios que puedan surgir en detrimento del Interés público, y es por ello por lo que es un factor clave que estos conocedores denuncien aquello que está pasando para poder prevenirlo o remediarlo, pudiendo así promover y/o garantizar el cumplimiento del Derecho y las políticas de la Unión.

Sin embargo, denunciar algo en una organización no estaba, y en muchas ocasiones sigue sin estarlo, bien visto, por lo que esos posibles denunciantes renunciaban a su derecho por miedo a las represalias que pudiera acarrear. De aquí se desprende la importancia de la existencia de canales de denuncia efectivos, confidenciales y seguros, y garantizar la protección efectiva de los denunciantes frente a consecuencias negativas.

2.2 Regulación Europea

2.2.1 Origen y motivación de la Directiva 2019/1937

Como se desprende del apartado anterior, socialmente, en los últimos años hay una creciente preocupación por los asuntos de corrupción sobretodo en el ámbito de la Unión Europea. Con objeto de facilitar la denuncia por parte de las personas que podrían alertar de estas conductas ilícitas es necesario solventar la falta de protección de los denunciantes, que ven como sufren represalias por sus denuncias.

Como ejemplo, hay dos casos que destacan y que servirán como precedentes para el impulso de la Directiva. Se tratan del caso GUJA contra Moldavia y el caso HALET contra Luxemburgo.

En el caso Guja, un trabajador de la Fiscalía General de la República de Moldavia fue despedido por manifestar a la prensa cómo un alto cargo político del Estado de Moldavia intervino en la tramitación de un proceso penal, intentando que se absolviera a cuatro policías por una denuncia de abusos policiales. La filtración se produjo después de que el presidente de la República, el señor Voronin, lanzara una llamada a la lucha contra la corrupción y contra aquellos abusos que pudieran ejercer los altos cargos.

Iacob Guja, el demandante, como apoyo a su denuncia, envió copia de dos cartas que tenía en su posesión, ya que habían sido enviadas a la Fiscalía General sin ninguna nota de confidencialidad, al diario *Jurnal de Chisinau.* Este se hizo eco de la noticia, publicando un artículo titulado “Vadim intimida a los fiscales”, que básicamente explicaba el caso de estos policías y otros casos en los que se intuía que había habido un tráfico de influencias para beneficiar a personas del interés del alto cargo.

Fue entonces cuando el Fiscal General le preguntó al señor Guja cómo la prensa había llegado a obtener esa información, y, tras un intercambio de cartas, acabó lanzando un mensaje donde viene a decir que fue él mismo quién filtró la información porque creía en el discurso anti-corrupción que había dado el presidente anteriormente y quería dejar a la Fiscalía en una buena posición. Poco más de dos semanas después, el señor Guja fue cesado del cargo por tener las cartas filtradas consideración de secretas y por no haber consultado con superiores de la Fiscalía si se podían o no transmitir. Es en este punto cuando el Sr. Guja interpone una acción civil para su readmisión en el cargo y argumenta que los documentos no son privados según la ley, que no existía la obligación de consulta

con los responsables antes de contactar con la prensa y que esa divulgación no afecta negativamente a sus empleadores. Tanto el tribunal de Apelación de Chisinau como el Tribunal Supremo rechazan sus apelaciones, alegando que no compete a la libertad de expresión la obtención de información a través de un abuso de sus funciones.

El caso se lleva en 2004 al Tribunal Europeo de Derechos Humanos (de ahora en adelante, TEDH), alegando que el derecho a la libertad de expresión que emane del artículo 10 del Convenio de Roma ha sido violado. Para juzgar si realmente este derecho debe prevalecer, el TEDH se centra en 6 puntos clave que luego servirán como precedentes para la Directiva.

Primero, se debe analizar si se tenían otros canales efectivos donde poder informar para remediar la situación. Seguidamente, se debe estudiar la importancia que tiene esa información para el interés general. También es importante estudiar la veracidad de esa información. Siguiendo el mismo hilo conductor, se debe analizar el perjuicio que puede conllevar para el empleador y, de la misma forma, si el denunciante actúa de buena fe o simplemente como reacción a algún interés oculto. Finalmente, se debe tomar en consideración cual ha sido la severidad de la acción de represalia contra el denunciante. Con el análisis hecho, el TEDH concluye que el demandante no disponía de otros medios para denunciar; que la información es de interés general, veraz, y que, por tanto, prevalece el interés general al perjuicio que puede provocar la falta de confianza del pueblo con la Fiscalía General; que el Sr Guja actúa de buena fe y que la sanción no es justificable.

Por todo ello, declara la demanda interpuesta por el Sr. Guja admisible y que hay una violación del artículo 10 del Convenio de Roma. Asimismo, impone una obligación al Estado de pagar una cuantía de dinero cercana a 20.000 euros al Sr. Guja en concepto de daños materiales, costas y gastos.

El siguiente caso por estudiar es el caso de Halet vs Luxemburgo, también conocido como el caso LuxLeaks, que culminó el pasado 14 de febrero de 2023 con una sentencia favorable para el denunciante, Raphaël Halet.

El señor Halet, consultor de PricewaterhouseCoopers, en adelante PwC, en Luxemburgo, junto con otro compañero, filtró a un periodista unos documentos que señalaban la manera en la que varias empresas de renombre internacional (como Ikea, Pepsi o Apple, entre otras) conseguían eludir sus impuestos. Se trataban de acuerdos confidenciales entre las autoridades de Luxemburgo y estas empresas, realizados a través de PwC, en los que se acordaba la tributación de esas empresas en el Gran Ducado a cambio de un tipo de tributación menor a la estipulada legalmente, lo que se conoce como evasión fiscal.

Esta información confidencial (documentos fiscales, declaraciones tributarias…) fue transmitida a un periodista que la estudió y publicó, y junto con la ayuda de otros periodistas de muchos otros países, destapó uno de los casos de evasión fiscal más sonados de la Unión Europea y que ha marcado un claro antecedente en contra de la corrupción.

Halet, el demandante, fue despedido por PwC. Fue condenado también penalmente por la justicia luxemburguesa, que no le concedió la condición de denunciante, a prisión y el pago de una multa, aunque, tras su recurso al Tribunal de Apelación, la represalia quedó en un pago de 1.000 euros. Se consideró que, pese a ser de interés general, no lo era lo suficiente como para contrarrestar el perjuicio que ocasionó a la empresa y, por tanto, el artículo 10 del Convenio de Roma no fue violado. Después de un recurso de casación que también resultó en un fracaso para la defensa del demandante, se interpuso una siguiente demanda ante el TEDH.

En un primer momento, en la sentencia de 2021, el tribunal daba la razón a la justicia luxemburguesa ya que optó por entender que la ponderación entre el interés general y la libertad de expresión y el daño causado a PwC era justa y, por tanto, no se vulnera el artículo 10. Es en la sentencia del 14 de febrero de 2023 cuando el TEDH cambia de opinión y da la razón al demandante, el señor Halet, condenando a los tribunales de Luxemburgo a pagar más de 50.000 euros al mismo.

Analizando la sentencia, podemos ver que se rige por la jurisprudencia de la sentencia Guja, comentada anteriormente. Entiende que la condición de *whistle-blower*, y, por tanto, la protección que se le ofrece, tiene que otorgarse según las características y contexto concreto del caso, y que el tribunal de Apelación nacional había fallado erróneamente, puesto que no consideró que el perjuicio causado a PwC no superaba el interés general, ya que contribuía innegablemente a proporcionar una nueva visión y un importante debate sobre la elusión de tributos, la exención y evasión fiscal a nivel nacional y europeo.

Si valoramos los seis puntos comentados en la sentencia Guja, vemos lo siguiente. Sí se dan correctamente en este supuesto, ya que, pese a que se le da prioridad al canal interno, entiende que la publicidad es la única alternativa realista para dar la voz de alerta. Se entiende también que la información es cierta, puesto que en ningún momento se ha puesto en duda la veracidad de la misma. La buena fe también se entiende, puesto que no buscaba un beneficio propio sino un beneficio para el público en general. Al estudiar el interés público que pueda generar, vemos que, pese a que ya se estaba investigando sobre el tema, el tribunal entiende que la información si conlleva un interés público, puesto que muestra las prácticas que llevan a cabo ciertas empresas en un entorno fiscal completo y saca a relucir la necesidad de reconducir esta situación ilegal. Valorando el perjuicio causado a PwC, el TEDH entiende que, pese a que es elevado, la necesidad de información sobre un tema tan relevante que puede poner en tela de juicio las relaciones entre empresas, clientes e instituciones gubernamentales prevalece sobre los daños que se pudiesen causar; finalmente, al analizar la severidad de la represalia hacia Halet, el tribunal la entiende como desproporcionada, teniendo en cuenta que el derecho a la libertad de expresión debería prevalecer.

Es por todo ello por lo que el Tribunal ha declarado de nuevo la violación del artículo 10 del CEDH relativo al derecho de la demandante a la libertad de expresión y a la libertad de información.

2.2.2 Aspectos fundamentales de la Directiva 2019/1937

El objeto de la Directiva es establecer unas normas comunes que doten a las personas que informen sobre infracciones del Derecho de la UE de un elevado nivel de protección.

El objeto de estas informaciones, como se ha mencionado, es cualquier situación que suponga, o al menos haya indicios y fundamentos para creer que es así, una vulneración del Derecho de la Unión. Es en el artículo 2 de la misma donde se delimita en ámbito de aplicación material y da la opción a los Estados miembros a ampliar la protección a otros ámbitos una vez hecha la transposición. Estos ámbitos, especificados en el anexo de la Directiva, se resumen en: contratación pública; servicios, productos y mercados financieros, prevención del blanqueo de capitales y financiación del terrorismo; seguridad de los productos y conformidad; seguridad del transporte; protección del medio ambiente; protección frente a las radiaciones y seguridad nuclear; seguridad de los alimentos y los piensos, sanidad animal y bienestar de los animales; salud pública; protección de los consumidores; protección de la privacidad y de los datos personales, y seguridad de las redes y sistemas de información; infracciones que afecten a los intereses financieros de la UE y, finalmente, infracciones relativas al mercado interior, incluidas las que infrinjan las normas europeas en materia de competencia y ayudas otorgadas por los Estados y aquellas que infrinjan las normas del impuesto de sociedades o busquen una ventaja fiscal sobre el mismo.

El concepto de denunciante que recoge la directiva es extenso, y comprende como mínimo a: trabajadores del sector público o privado; a aquellos cuya información la obtuvieran de una relación laboral ya finalizada; a aquellos cuya relación laboral no haya sido iniciada pero hayan obtenido la información durante el proceso de selección o negociación contractual; y a facilitadores, terceros que tengan relación con el denunciante, como familia o compañeros, y puedan sufrir represalias en un contexto laboral y las entidades jurídicas propiedad del informante, para la cual trabajen o mantenga otro tipo de conexión laboral.

En este sentido, se entenderá como trabajador como mínimo a los funcionarios y personas que tengan condición de trabajador según apartado 1 del artículo 45 del TFUE; trabajadores no asalariados según el artículo 49 TFUE; accionistas y personas que pertenezcan al órgano de administración, dirección o supervisión de una empresa, incluidos los miembros no ejecutivos, así como voluntarios y trabajadores en prácticas, perciban o no una remuneración; y a cualquier persona que trabaje bajo la supervisión y dirección de contratistas, subcontratistas y proveedores.

Estos denunciantes gozarán de la protección siempre que tengan motivos razonables para pensar que la información es veraz, que entra en el ámbito de aplicación de la Directiva y hayan efectuado la denuncia por alguno de los tres canales que la misma dictamina: canales internos, siguiendo el artículo 7; revelación pública, siguiendo el artículo 15; o canales externos, siguiendo el artículo 10. Aquellos denunciantes que lo hagan ante alguna institución, órgano u organismo que pertenezca a la UE, tendrán el mismo derecho a protección que si lo hubiesen hecho frente a un canal externo.

La Directiva también deja entender que debería haber un orden de elección de los sistemas, aunque no obligatorio, parece que se entiende como el adecuado. El principal debe ser el canal de denuncias interna y, en caso de no poderse usar por miedo a represalias o no garantice el tratamiento efectivo de las denuncias, será cuando se usará el canal externo de denuncias. Para estos dos niveles, el legislador europeo especifica que hay un deber de confidencialidad por el que no se debe revelar la autoría de la denuncia a menos que exista una autorización expresa por parte del denunciante. También que los datos personales se deberán tratar de conformidad con el Reglamento UE 2016/679 y la Directiva UE 2016/680 y que las denuncias deberán quedar registradas y se conservarán durante el tiempo necesario para cumplir los requisitos impuestos por la misma. El tercer nivel será analizado posteriormente.

Pese a que para los sistemas de denuncia internos y los externos (artículos 9.1.a y 12.1.a), se exige la garantía de confidencialidad de la identidad del denunciante, no se exige el anonimato, que deja a libre elección de los Estados miembros. En todo caso, sí indica que, en caso de que la denuncia sea anónima y posteriormente se identifique al responsable, éste gozará de la misma protección.

Como se ha comentado anteriormente, el sistema de denuncias se articula con 3 niveles diferentes.

El primer nivel es el canal de denuncias internas, regulado en el Capítulo II de la Directiva. Indica que los Estados miembros deben promover la comunicación a través de este canal, que debe permitir a los trabajadores comunicar información sobre infracciones, antes de las otras posibilidades, siempre que se pueda garantizar el tratamiento de las denuncias de manera efectiva y el denunciante crea que no hay riesgo de represalias. Esta comunicación puede realizarse de forma escrita o verbal, ya sea por vía telefónica, por otros sistemas de mensajería o incluso, a solicitud del denunciante, a través de una reunión presencial.

La obligación es para todas las entidades jurídicas privadas que tengan 50 o más trabajadores y para todas las entidades jurídicas públicas. En el sector público, deja a los estados miembros la decisión arbitraria de eximir de esta responsabilidad a los municipios con menos de 10.000 habitantes y/o a las entidades con menos de 50 trabajadores.

Prevé que estos canales deben gestionarse o bien por una persona o departamento designados o bien externamente por un tercero y que, en caso de entidades privadas que

tengan entre 50 y 249 trabajadores, pueden compartir recursos para recibir e investigar denuncias.

Estos canales deben estar diseñados y gestionados de una forma que garantice la confidencialidad de la identidad del denunciante y de cualquier tercero mencionado, y debe impedir el acceso a personal no autorizado. Se debe realizar un acuse de recibo de la denuncia en un plazo de 7 días a contar desde la recepción de la misma. La persona o departamento que se encargue de la tramitación de las mismas (ya sea la recepción o el seguimiento) debe ser imparcial y debe realizar un seguimiento diligente y debe dar respuesta en un plazo no superior a 3 meses a contar del acuse de recibo.

El segundo nivel es el canal de denuncias externas, regulado en el Capítulo III. Cada Estado miembro debe designar quién será autoridad competente para recibir, seguir y responder las denuncias, así como dar recursos suficientes y adecuados. Estas autoridades deberán establecer canales de denuncia independientes y autónomos, seguir las denuncias diligentemente y, como en el caso del canal interno, dar acuse de recibo en el plazo de siete días y responder al denunciante en un plazo menor a 3 meses. En caso de que la autoridad reciba una denuncia para la que no tenga competencias, deberá ser transmitida al órgano correspondiente.

Se entiende que los canales son independientes y autónomos cuando en su diseño y gestión se garantice la exhaustividad, integridad y confidencialidad de la información y permita el almacenamiento duradero de información para posibles nuevas investigaciones posteriores. Igual que en el caso del canal interno, las denuncias podrán ser escritas o verbales, aceptando también reuniones presenciales. Insta además a que, en caso de que la denuncia sea recibida por un canal que no sea el establecido, o por un miembro que no sea el responsable del tratamiento, estos deberán mantener el deber de confidencialidad y trasladar al menos tardar posible la denuncia al responsable.

La Directiva dota de competencia a los Estados miembros a permitir a sus autoridades competentes a finalizar el seguimiento del caso, después de su estudio y argumentación, cuando sea una infracción menor que no necesita seguimiento o a archivar el procedimiento en caso de que las denuncias sean reiteradas y no aporten información nueva, siempre que los procedimientos anteriores al archivado hayan concluido.

Son también los Estados miembros los que deberán garantizar que las autoridades designadas publiciten y publiquen de una forma accesible la siguiente información: condiciones para acogerse a la protección, datos de contacto; procedimiento aplicable al sistema, indicando como se puede solicitar más información o los plazos que deberá seguir; régimen de confidencialidad y protección de datos aplicable; las vías de recurso frente a represalias; y una declaración en la que se explique las condiciones de protección para no incurrir en responsabilidad por infringir alguna norma de confidencialidad o de revelación de información.

El tercero es la revelación pública, regulado en el Capítulo IV de la Directiva. Este nivel puede considerarse de carácter residual, en cuanto a que solo está permitido en casos concretos. Solo cuando ninguno de los dos canales anteriores haya sido efectivo en cuanto al plazo de respuesta o cuando el denunciante tenga motivos suficientemente razonables para pensar que o bien la infracción constituya un peligro inminente al interés público o bien haya un riesgo de represalias o de poca efectividad de la denuncia en caso de denuncia externa. Entiende poca efectividad en el sentido de poca posibilidad de que se dé un tratamiento fiable por motivos como ocultación de pruebas o afinidad del denunciado con la autoridad competente, ya sea por conveniencia o por implicación en la infracción.

Los Estados miembros tendrán que velar por asegurar que no existen represalias ni amenazas ni tentativas de las mismas, en particular en forma de suspensión, despido, destitución o medidas equivalentes; degradación o denegación de ascensos; cambio de puesto de trabajo, lugar o reducción salarial; denegación de información; evaluación o referencias negativas; imposición de cualquier medida disciplinaria, incluidas sanciones pecuniarias; coacciones, intimidaciones o acoso; discriminación o trato desfavorable; no conversión de un contrato de trabajo temporal en indefinido en caso de expectativas legítimas de que ocurriría; no renovación o terminación anticipada de un contrato de trabajo temporal; daños a su reputación; inclusión en las listas negras sobre la base de un acuerdo que pudiese implicar dificultad para encontrar otro empleo en el sector; terminación anticipada o anulación de contratos de bienes o servicios; anulación de licencia o permisos; y referencias médicas o psiquiátricas. La carga de la prueba en este aspecto está invertida, es decir, se presumirá que el acto ha sido consecuencia de la denuncia y será quien ha tomado alguna de estas acciones contra un trabajador con protección como denunciante quién deba probar que la motivación de la acción es otra diferente.

Serán también los Estados miembros quién deberán proporcionar información y asesoramiento completo sobre los procedimientos y recursos disponible para la defensa del denunciante, así como asistencia jurídica penal y a los procedimientos civiles transfronterizos de conformidad con la Directiva (UE) 2016/1919 y la Directiva 2008/52/CE, y el acceso a la asistencia jurídica en ulteriores procedimientos y asesoramiento jurídico u otra asistencia jurídica de conformidad con la legislación nacional, así como asegurarse de que goza plenamente del derecho a la tutela judicial efectiva y un juez imparcial. Deja la puerta abierta también a que puedan prestar asistencia financiera y psicológica a los denunciantes en el marco de un proceso judicial.

Los denunciantes no incurrirán en un delito de revelación pública siempre que comuniquen de forma acorde al procedimiento de la directiva y lo hagan de buena fe, con un pensamiento razonable de que la información es veraz. Tampoco incurrirán en responsabilidad respecto a la adquisición o acceso a la información, a menos que de por si constituya un delito. En ese caso, se juzgará siguiendo el Derecho nacional aplicable.

Los Estados miembros deberán imponer sanciones efectivas con la intención de disuadir a aquellas personas físicas o jurídicas que impidan o intenten impedir la denuncia; adopten medidas de represalias contra un denunciante o promuevan procedimientos abusivos contra los mismos; y contra aquellos que no cumplan el deber de confidencialidad de la identidad de los denunciantes.

Asimismo, deben proponer sanciones para aquellos denunciantes que actúen de mala fe, cuando la información que comuniquen o publiquen sea falsa y se pueda demostrar que tenían conocimiento de ello, así como indemnizaciones por daños para aquellos afectados por la divulgación.

III. ANÁLISIS JURÍDICO DE LA LEY 2/2023

3.1 Transposición de la directiva en España

La obligación de España de transponer las directivas europeas es un elemento fundamental en su papel como Estado miembro de la Unión Europea. Transponer implica un proceso por el cual España incorpora a su ordenamiento jurídico interno las disposiciones y principios delineados en la directiva, con el fin de armonizar y coordinar las políticas del ámbito europeo.

Como podemos observar en la Disposición final de la directiva, el plazo máximo de transposición era el 17 de diciembre de 2021; sin embargo, en España, la ley que transpone la Directiva es del 2 de febrero de 2023, más de un año después del plazo establecido, hecho que puede conllevar a una sanción por parte de la UE.

En enero de 2022, la Comisión Europea inició un procedimiento contra España (INFR(2022)0073) por la infracción de no transposición de la Directiva. En julio de 2022, la Comisión emitió un dictamen motivado (tanto a España como a quince otros estados miembros) por no haber comunicado medidas para la plena transposición de la Directiva. Pese a que a inicios de febrero de 2023 se aprobó la norma española que transponía la Directiva, poco tiempo después la Comisión inició un procedimiento de infracción ante el TJUE contra 8 estados miembros, entre ellos España, por incumplimiento del Derecho de la Unión en la transposición de esta Directiva, dado que creen que la respuesta de estos estados a los dictámenes motivados no fue satisfactoria.

Tendremos que esperar a ver cuál es el resultado de este procedimiento, de importancia relevante, puesto que la última multa impuesta a España en un procedimiento parecido fue de 15 millones de euros.[1]

Veo importante remarcar que la transposición de la norma debe tener no solo un carácter de forma sino de fondo, en el sentido en que la norma estatal debe perseguir los mismos objetivos que la Directiva, sin descontextualizar el propósito, y la UE debe velar por ello.

Se puede ver prueba de ello en el caso de Hungría. Como en el caso de España, la Comisión ha dado traslado de su expediente al TJUE, no solo por la tardanza en la transposición sino por el mal uso que se le da, o puede darse, a de los canales establecidos por la Directiva. Actualmente, el canal se está usando para informar a las autoridades de acciones que van en contra del pensamiento conservador que reina en el país, hecho que pone en peligro los avances progresistas que se han llevado a cabo y que, en ciertos casos, puede ir en contra de los derechos humanos. Hablamos de denuncias, por ejemplo, a

[1] MIRANZO DÍAZ, J. "La nueva Directiva europea de protección del denunciante: un análisis desde el derecho público" *Revista General de Derecho Europeo*, 49, 2019.

personas del colectivo LGTBIQ+ o a familias que viven sin seguir el esquema de familia tradicional.[2]

3.2 Nueva Ley 2/2023

3.2.1. Finalidad de la ley y ámbitos de aplicación

La finalidad de la ley es, por un lado, proteger adecuadamente a las personas físicas frente a las posibles represalias que podrían sufrir en caso de informar sobre alguna acción u omisión que puedan constituir infracciones del Derecho de la Unión Europea de la que tengan conocimiento y, por otro lado, 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. Para ello, se servirá de dos grandes herramientas: el sistema interno de información dentro de la propia organización y el canal externo de información, que será llevado a cabo a través de la Autoridad Independiente de Protección del Informante (en adelante A.A.I.)

Protegerá a los informantes que trabajen en el sector público o privado e informen sobre acciones u omisiones que puedan constituir infracciones del Derecho de la Unión Europea, u aquellas que puedan constituir infracción penal o administrativa grave o muy grave, como pueden ser las infracciones del tipo que impliquen quebranto económico para la Hacienda Pública y/o la Seguridad Social.

Para concretar aquello que se entiende como infracción del Derecho de la UE, encontramos tres situaciones diferentes. La primera, que entre dentro del ámbito de aplicación de los actos de la UE, coincidiendo con aquellos mencionados *ad supra* en el apartado donde se analiza la Directiva; la segunda, que afecte a los intereses financieros de la UE y; la tercera, que incida en el mercado interior, incluyéndose aquí las infracciones de las normas de la UE en materia de competencia y el otorgamiento de ayudas nacionales, así como aquellas relacionadas con la infracción de la normativa sobre impuestos de sociedades u otras ventajas fiscales.

La norma excluye aquellas informaciones relativas a infracciones en la tramitación de procedimientos de contratación que contengan información clasificada o declarada secreta o reservada.

Para que pueda ser considerado informante, la persona física debe trabajar en el sector público o privado y debe haber obtenido la información en un contexto laboral o profesional. A tales efectos, se considerará informante si tiene condición de empleado público o por cuenta ajena; los autónomos; los accionistas, partícipes o pertenecientes al órgano de administración; aquellos que trabajen para o bajo la supervisión y dirección de

2 Le Monde with AFP, Hungary strips 'anti-LGBTQ' section from whistleblower law. (Mayo 2023).

contratistas, subcontratistas o proveedores; voluntarios, becarios, trabajadores en periodo de formación, facilitadores. La ley se aplicará por defecto a aquellos que mantengan la relación, aquellos cuya relación laboral o estatutaria ya haya finalizado y a aquellos que a hayan obtenido durante el proceso de selección o de negociación precontractual pese a que la relación laboral todavía no haya comenzado. Igual que en la Directiva, también quedaran cubiertos por las medidas de protección del informante aquellas personas físicas que tengan una relación con el informante de compañeros de trabajo o familia; aquellos conocidos como facilitadores; y aquellas personas jurídicas con quien mantenga una relación en un contexto laboral.

3.2.2 Sistema interno de información

La Directiva marca que los estados miembros deben promover el uso del canal de denuncia interna por encima del canal externo. Así lo hace al artículo 4 de la presente Ley, donde dice, y cito textualmente, es el *"*cauce preferente para informar sobre las acciones u omisiones previstas…*"*[3].

Será el órgano de administración o de gobierno de cada entidad el responsable de implantar el sistema, así como de designar a la persona que tomará el rol de "Responsable del Sistema". El propósito de este sistema es que todas aquellas personas recogidas en el ámbito personal puedan informar de forma segura, garantizando la confidencialidad de su identidad y la de los terceros mencionados. Las comunicaciones se deben tratar de manera efectiva. Para ello, deben enunciar y publicitar una política en la que la independencia y diferenciación respecto a los sistemas internos de otros organismos deben estar presentes.

Este canal interno de información puede ser llevado a cabo por un tercero externo, siempre que ofrezca las garantías adecuadas en materia de independencia, confidencialidad, protección de datos y secreto de comunicaciones, es decir, no puede menoscabar las garantías y requisitos necesarios para el sistema interno. Esta posibilidad no tiene restricciones en el sector privado. En cambio, en el sector público, solo será posible cuando se acredite insuficiencia de medios propios y, en todo caso, el tercero solo gestionará la recepción de denuncias, con carácter puramente instrumental.

Las comunicaciones se pueden hacer de manera escrita, por correo postal o algún medio electrónico habilitado para ello; o verbal, ya sea por vía telefónica, mensajería de voz o incluso de forma presencial, para lo que en el plazo de 7 días desde su notificación, el responsable del canal debe concertar una reunión. La información recabada, ya sean grabaciones, transcripciones o actas (que el denunciante podrá firmar y rectificar), se almacenarán, igual que los datos personales relativos a la mismas, durante el periodo que sea estrictamente necesario y proporcionado al cumplimiento de la Ley.

[3] 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, articulo 4

Como se ha anticipado anteriormente, es el órgano de administración o de gobierno el encargado de la designación como "Responsable del Sistema" a una persona física (o a un órgano colegiado, en cuyo caso uno de los miembros será el delegado) así como de su destitución o cese. Estos actos deberán informarse a la A.A.I. o a la autoridad competente de la comunidad autónoma; en el caso de Cataluña, a la Oficina Antifrau (https://www.antifrau.cat/ca/autoritat-competent-proteccio-persones-alertadores).

El Responsable del Sistema debe actuar de forma independiente y autónoma, por ello no puede recibir instrucciones en su ejercicio y se le debe dotar de medios suficientes para llevar sus funciones a cabo.

El sistema de información interno debe cumplir unos requisitos mínimos en cuanto al proceso de gestión de la información que se recibe. Primero de todo, debe identificarse y publicitarse claramente, así como informar de las posibilidades de denuncia que brinda también el canal externo ante las autoridades competentes. Seguidamente, el Responsable del Sistema debe ser un directivo de la entidad que pueda trabajar de forma independiente del órgano de gobierno y, si no fuese posible por motivos de naturaleza o dimensión, para evitar posibles conflictos de interés, se podría designar a otra persona para ello. Una vez el denunciante hace eco de su información a través de este canal, se le debe, en un plazo máximo de 7 días, enviar un acuse de recibo, a menos que pueda poner en peligro su confidencialidad.

El Responsable del Canal debe investigar y en un plazo máximo de 3 meses a contar a partir del envío del acuse, debe dar una respuesta al denunciante, salvo en casos de especial complejidad, donde el plazo puede llegar a ser de 6 meses.

Se deberá avisar a la persona afectada de las acciones u omisiones que se le atribuyen y tiene derecho a ser escuchada en cualquier momento, así como en el canal se debe respetar su derecho al honor y a la presunción de inocencia.

Dentro del sistema interno de información, hay algunas especificidades con relación a si se trata en el sector privado o el público, como son las entidades obligadas o la posibilidad de recursos compartidos.

3.2.2.1 Privado

Aquellos obligados a tener al alcance de los recogidos en el ámbito personal de esta norma aquellas personas físicas o jurídicas que tengan contratados a 50 o más trabajadores; los partidos políticos, sindicatos, organizaciones empresariales o fundaciones creadas por estos, cuando reciban o gestionen fondos públicos; y las personas jurídicas que, independientemente del número de trabajadores, entren en el ámbito de aplicación de ciertos actos de la Unión Europea, como pueden ser la protección del medio ambiente, la prevención del blanqueo de capitales o la financiación del terrorismo, entre otros.

En el caso concreto de que se trate de una persona jurídica que tenga entre 50 y 249 trabajadores, podrá compartir el Sistema interno de Información, así como sus recursos, con otras figuras de su mismo género, siempre que se garanticen las premisas establecidas por la norma para aquellas figuras que no compartan recursos.

3.2.2.2 Público

En el caso de las entidades que integran el sector público, no existe un requisito mínimo de trabajadores para la obligación de disponer de un Sistema interno de información. Se entiende que integran el sector público la Administración (estatal, autonómica y local), los organismos y entidades públicas vinculadas a la misma, el Banco de España y el organismo de Seguridad Social, las universidades públicas, las corporaciones de Derecho público, las fundaciones del sector público y las sociedades mercantiles cuyo más del 50% del capital social corresponda a alguna de las mencionadas anteriormente, así como los órganos constitucionales. En caso de organismos públicos dotados de competencia para ser Autoridades Independientes, deberán tener un canal interno diferenciado para las denuncias referentes a los propios incumplimientos del organismo y otro canal para las denuncias de terceros cuya investigación sea su competencia.

Siguiendo con la diferenciación del sector público del privado, en este caso refiriendo a los medios compartidos, podrán compartir bajo la misma premisa de garantía del buen funcionamiento del sistema aquellos municipios de menos de 10.000 habitantes (si comparten comunidad autónoma) y aquellas entidades pertenecientes al sector público con personalidad jurídica propia pero vinculadas o dependientes de la administración territorial que cuenten con menos de 50 trabajadores.

3.2.3 Canal externo de información de la Autoridad Independiente de Protección del Informante

La norma, en su artículo 16, aporta la posibilidad a toda persona física a informar sobre acciones u omisiones amparadas en el ámbito material de la Ley ante la Autoridad Independiente de Protección del Informante, en adelante AAI. Aquello aplicable a la AAI también lo será a las autoridades autonómicas competentes, en el caso de Cataluña, la *Oficina Antifrau.*

La información puede revelarse de manera anónima y, si no fuese así, el informante tiene derecho a que su identidad no sea revelada a terceras personas. Para ello, se deberán utilizar métodos adecuados. Sólo en caso de investigación penal, disciplinaria o administrativa deberá ser revelada a la Autoridad judicial competente.

De igual forma que para el canal interno, debe haber opción a revelar la información de manera verbal, presencial o escrita. Una vez presentada, se registrará en el Sistema de Gestión de Información, asignándosele un código de identificación, que deberá figurar junto a la fecha de recepción, las actualizaciones desarrolladas, las medidas adoptadas y,

finalmente, la fecha de cierre. En este sentido, el informante deberá recibir el acuse de recibo en un plazo máximo de 5 días hábiles a contar desde la recepción.

En un plazo no superior a 10 días hábiles desde la recepción, la AAI deberá analizar si la información entra dentro del ámbito de aplicación de la Ley 2/2023 e informar al denunciante sobre la decisión que se tome. Se podrá:

- Inadmitir la comunicación, en caso de que los hechos carezcan de credibilidad; en caso de que la comunicación no tenga fundamento o existan sospechas sobre la comisión de un delito para obtener la información; cuando los hechos no constituyan una infracción o; finalmente, cuando la comunicación no tenga información nueva y ya se haya investigado el caso.
- Admitir a trámite la comunicación, en un plazo no superior a 5 días hábiles.
- Remitir la comunicación al Ministerio Fiscal, cuando los hechos sean constitutivos de delito; o a la Fiscalía Europea, en caso de afectación a los intereses financieros de la UE.
- Remitir la comunicación a la autoridad competente.

Debe proceder entonces a la instrucción del caso. La persona afectada debe ser informada y se le permitirá hacer alegaciones escritas, pero nunca se le revelará la identidad del informante ni se dará acceso a la información. Una vez finalizada la instrucción, que no debe ser superior a 3 meses, se debe emitir un informe en el que figure la exposición de los hechos relatados, la clasificación de la comunicación, las actuaciones realizadas y finalmente, las conclusiones alcanzadas. Este informe servirá a la AAI para archivar el expediente, remitirlo al Ministerio Fiscal en caso de ver indicios de delito, trasladarlo a la autoridad competente o iniciar un procedimiento sancionador. Este procedimiento de instrucción debe ser revisado cada 3 años.

La ley otorga unos derechos y garantías al informante ante la AAI. Este puede decidir si quiere informar de manera anónima o no, pese a que en ese caso de debe garantizar la confidencialidad de la identidad; informar escrita o verbalmente; indicar un domicilio o correo electrónico para recibir las comunicaciones o incluso renunciar a recibir comunicaciones; comparecer ante la AAI por propia iniciativa o siendo requerido para ello con su abogado, incluso por videoconferencia; ejercer los derechos que le concede la legislación en materia de protección de datos y, finalmente, conocer el estado de la tramitación de la denuncia y los resultados de la misma. [4]

3.2.4 Publicidad y registro de la información

Los sujetos obligados por la norma (organizaciones, empresas, fundaciones…) deberán proporcionar información clara y accesible a los informantes en potencia. En caso de que

[4] 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, articulo 21

tengan página web, deberá constar en ella. La Autoridad Independiente de Protección del Informante y sus homólogos en las comunidades autónomas deberán, en su sede electrónica, informar de: las condiciones para acogerse a la protección, los datos de contacto, los procedimientos de gestión por los que se rigen, el régimen de confidencialidad aplicable y las vías de recurso frente a represalias.

Aquellos sujetos obligados a disponer de un canal interno de denuncias deberán, además, contar con un libro registro de carácter confidencial de las informaciones y de las investigaciones internas que hayan llevado a cabo.

3.2.5 Revelación pública

La revelación pública se entiende como la puesta a disposición del público de información sobre acciones u omisiones. Se podrán acoger a la misma protección a las mismas medidas de protección que aquellos que informarán por el canal interno y externo siempre que se cumpla alguna de las siguientes condiciones:

- Que previamente se haya comunicado a través del canal interno y externo (o solamente por el externo) y no se hayan tomado medidas apropiadas en el plazo establecido
- Que se tengan razones para creer que o bien el peligro es inminente o manifiesto para el interés público, o bien existe un riesgo de represalias o haya pocas probabilidades de tratamiento si se denunciara por alguno de los otros canales.

Estos requerimientos no son necesarios para aquellos que revelen la información directamente a la prensa, con arreglo al ejercicio de la libertad de expresión y de información veraz, previstas constitucionalmente.[5] En este caso se deberá aplicar las medidas de protección que se explican posteriormente en el apartado 3.4

3.2.6 Medidas protección

La Ley protege a aquellos de informen a través de alguno de los canales destinados a ello, siempre que se cumplan los requerimientos en la misma y que se tengan motivos razonables para pensar que la información que transmiten es veraz. En este sentido, quedan expresamente excluidos aquellos que revelen información sobre algún conflicto interpersonal entre denunciante y denunciado, aquellas informaciones que ya sean disponibles para el público; aquellas que se refieran a ámbitos no previstos en la norma; y aquellas que ya hayan sido inadmitidas por las causas mencionadas en el punto 3.2.3.

[5] 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, articulo 28.2

Para proteger al informante, se prohíben expresamente los actos considerados represalia, entendidos como actos u omisiones que estén prohibidos por ley o que afecten, directa o indirectamente, desfavorablemente a aquellos que se consideren informantes.

Según el punto 3 del artículo 36, se considerarán represalias:

a) Suspensión del contrato de trabajo, despido o extinción de la relación laboral o estatutaria, incluyendo la no renovación o la terminación anticipada de un contrato de trabajo temporal una vez superado el período de prueba, o terminación anticipada o anulación de contratos de bienes o servicios, imposición de cualquier medida disciplinaria, degradación o denegación de ascensos y cualquier otra modificación sustancial de las condiciones de trabajo y la no conversión de un contrato de trabajo temporal en uno indefinido, en caso de que el trabajador tuviera expectativas legítimas de que se le ofrecería un trabajo indefinido; salvo que estas medidas se llevaran a cabo dentro del ejercicio regular del poder de dirección al amparo de la legislación laboral o reguladora del estatuto del empleado público correspondiente, por circunstancias, hechos o infracciones acreditadas, y ajenas a la presentación de la comunicación.
b) Daños, incluidos los de carácter reputacional, o pérdidas económicas, coacciones, intimidaciones, acoso u ostracismo.
c) Evaluación o referencias negativas respecto al desempeño laboral o profesional.
d) Inclusión en listas negras o difusión de información en un determinado ámbito sectorial, que dificulten o impidan el acceso al empleo o la contratación de obras o servicios.
e) Denegación o anulación de una licencia o permiso.
f) Denegación de formación.
g) Discriminación, o trato desfavorable o injusto.

El periodo de protección de la Ley es de 2 años, prorrogable a petición del informante que viera sus derechos lesionados. Mencionar también que todos los actos que tengan intención de dificultar o impedir la presentación de las informaciones, tendrán consideración de nulos de pleno derecho.

Aquellos que tengan la consideración de informantes tendrán derecho a diferentes medidas de apoyo. Entre ellas se encuentran la asistencia efectiva por parte de las autoridades para garantizar la protección frente a represalias, la asistencia jurídica en los procesos penales y el apoyo financiero y psicológico, así como la asistencia jurídica gratuita.

3.2.7 Autoridad Independiente de Protección del Informante, A.A.I

Se define como ente de derecho público de ámbito estatal con personalidad jurídica propia y plena capacidad pública y privada, que actúa con independencia orgánica y funcional del Gobierno. Será el ente encargado de gestionar el canal externo de comunicaciones, adoptar las medidas de protección al denunciante, tramitar los procedimientos sancionadores y fomentar la cultura de la información.

3.2.8 Régimen Sancionador

La autoridad con competencias para sancionar es la Autoridad Independiente de Protección al Informante, otorgada por el artículo 61 de la presente Ley. Todas las personas físicas o

jurídicas que realicen actuaciones que se califiquen en la norma como infracciones, estarán sujetas al régimen sancionador.

Estas infracciones, descritas en el artículo 63 de la Ley 2/2023, se podrán calificar en muy graves, graves y leves, y acarrearán sanciones en función de que calificación se les den. Se encuentran detalladas en el artículo 65 de la norma.

3.2.9 Plazos de implementación

La Ley entra en vigor el 13 de marzo del 2023, 20 días después de la publicación de la misma en el BOE.

El plazo para implantar el Sistema interno de información será de máximo 3 meses para las todos los obligados a tenerlo excepto para las entidades jurídicas privadas que tengan menos de 249 trabajadores y para aquellos municipios que tengan menos de 10.000 habitantes. En estos casos, el plazo máximo se alarga hasta el 1 de diciembre de 2023.

3.3 Ley VS Directiva; invocación de la aplicación directa de la Directiva

Como podemos observar tras el análisis de ambas legislaciones, hay ciertas discrepancias entre la norma española y la Directiva Europea de la que proviene, siendo la primera más restrictiva.

En estos supuestos existen diversas posibilidades para que la protección sea aquella otorgada por la normativa europea en cuanto al principio de primacía de la legislación comunitaria.

Entre ellos destacan los expuestos en el presente apartado:

- Primacía del derecho de la Unión Europea

En este supuesto, en caso de conflicto entre una norma nacional y una norma europea, el Derecho de la UE tiene prevalencia sobre los Derechos internos de los Estados Miembros en caso de conflicto en el marco de las competencias de la Unión.

Dicho principio así se consagra en la Sentencia Costa/Enel del 15 de julio de 1964, por ello, cualquier norma europea prevalece sobre cualquier norma nacional, incluida la de rango constitucional siempre que se trate de un ámbito de competencia de la UE.

Por tanto, el alcance es absoluto, incluso sobre normas constitucionales (Sentencia Melloni, de 26 de febrero de 2013; STC 26/20014).

La principal consecuencia del principio de primacía del DUE es la inaplicación de la norma nacional contraria a la norma comunitaria “por su propia autoridad”.

Ahora bien, la inaplicación de la norma nacional no es la única consecuencia que se deriva del principio de primacía del Derecho de la Unión Europea: otra consecuencia es el hecho que el legislador o el autor de la norma interna debe solicitar o derogar dicha norma por ser contraria a la norma comunitaria; el juez no está facultado para ello, pero el el legislador (si es una ley) o el gobierno (si es un reglamento) sí. Este método es un control difuso y una forma de protección por las garantías europeas puesto que cualquier poder público tiene que aplicar el derecho comunitario sin tener que acudir a un tribunal europeo. Es relevante porque garantiza la uniformidad del derecho comunitario y permite mayor agilidad.

El juez nacional encargado de aplicar en el marco de su propia competencia la disposición del Derecho Comunitario tiene la obligación de asegurar el pleno efecto de esas normas, dejando inaplicada, si es preciso, y por su propia autoridad, cualquier disposición contraria de la legislación nacional.

Por ello, en el caso que una Ley sea contraria a la UE, el Tribunal Constitucional, aceptando lo que dijo el TJUE en el auto 168/2016, determina que hay que dar prioridad a la cuestión prejudicial, explicada más adelante en el apartado, y dar preferencia a los mecanismos de solución de conflictos previstos por la Unión Europea.

En el caso concreto de la Directiva 2019/1937 y la Ley 2/2023, la primacía del derecho de la UE haría referencia a que un trabajador que informe de una irregularidad tiene derecho a que se le exima de cualquier responsabilidad, incluso la penal, en caso de que la denuncia sea de buena fe y siga alguno de los procedimientos marcados por la norma, tal y como dice el artículo 21.2 de la Directiva, pese a que en el artículo 38.1 de la Ley 2/2023 española, no se exima al informante de responsabilidad penal.

- Aplicación directa de la Directiva

La aplicación directa dentro del sistema legal es la aptitud del Derecho de la Unión Europea para crear derechos y obligaciones directamente, por sí mismo, a los particulares y a los Estados Miembros.

No se debe confundir con la RECEPCIÓN AUTOMÁTICA puesto que hace referencia a que el Derecho de la Unión, cuando entra en vigor de acuerdo con los procedimientos correspondientes, es Derecho de los Estados Miembros; ni con la APLICABILIDAD DIRECTA, aunque es cierto que tienen mucho que ver, puesto que hace referencia a que existen normas europeas que por su naturaleza son *self-executing*; son autosuficientes, se bastan a sí mismas para desplegar efecto y, no hace falta que sean complementadas por otras normas; internas o de la Unión Europea.

Según la jurisprudencia del TJUE, para que una disposición de una norma comunitaria tenga efecto directo, hace falta que la norma sea clara, que no contenga ambigüedades en cuanto a su tenor imperativo y en cuanto a su objeto sea deducible fácilmente por el juez ordinario. Asimismo también requiere que la norma sea suficientemente precisa, en el

sentido que pueda afirmar sin duda alguna que la norma otorga un derecho a un particular o le impone una obligación. Finalmente, se requiere que la norma sea incondicional y que no esté sujeta a condición o reserva, como puede ser un plazo.

En este supuesto, las Directivas son una norma que no es aplicable directamente, puesto que les concede a los Estados un plazo para que adopten las medidas que requieren de su ejecución.

Las Directivas europeas exigen a los Estados que adopten medidas en este plazo, en consecuencia, la norma europea no es aplicable directamente y pide la intervención de los Estados o de las Instituciones europeas. Ahora bien, el TJUE ha determinado que las Directivas pueden tener EFECTO DIRECTO VERTICAL ASCENDENTE: un particular puede invocar lo que disponga la Directiva a su favor frente al estado, pero el Estado no puede exigir a un particular que cumpla lo esgrimido en la Directiva ni tampoco se pueden invocar en las relaciones entre particulares (efecto horizontal).

En el caso concreto de la Directiva 2019/1937 y la Ley 2/2023, el efecto directo de la Directiva de la UE haría referencia a que un trabajador que informe de una irregularidad no le puede exigir a la empresa que no presente cargos penales sobre él mismo por algún delito, como revelación de secretos, porque la normativa española, en su artículo 38, no exime de responsabilidad penal al informante pero, sin embargo, el trabajador podría, en sede judicial, pedir que se aplique el artículo 21.2 de la Directiva, que exime de toda responsabilidad al denunciante, siempre que la denuncia sea de buena fe.

En caso de que al juez *a quo* le sura alguna duda sobre la aplicación de este derecho comunitario, se deberá plantear una cuestión prejudicial, explicada al final de este apartado.

- Principio de interpretación conforme

La interpretación conforme del derecho nacional con el derecho de la Unión Europea (Sentencia Von Colson, de 10 de abril de 1984) consiste en la obligación de interpretar el Derecho nacional "a la luz de la letra y la finalidad" de la norma de la UE (efecto transfusión o inclinado). Es decir, en lugar de inaplicar directamente una norma interna que pueda ser contraria a una comunitaria, se debe intentar hacer una interpretación conforme de la norma nacional con la europea, si la interpretación es posible; aplicamos la norma nacional con arreglo a lo que disponga la norma europea, si bien existen límites que se deben respetar en esta interpretación conforme.

Los requisitos para que pueda proceder esta interpretación conforme son que haya una norma nacional que pueda ser interpretada, que la interpretación de la norma nacional sea razonable ("en la medida de lo posible" y que "no sea en contra del sentido natural de toda interpretación") y que la interpretación de conformidad de una norma interna con una

norma comunitaria no pueda llevar a establecer responsabilidad penal o agravar la responsabilidad penal de un particular.

En este sentido, no se debe nunca dejar de tener la mira puesta en que es una directiva que se ha hecho no solo en contra de la corrupción, sino para proteger el Derecho de la Unión Europea. En este mismo sentido, la protección al denunciante es lógica porque, en caso contrario, no existirían denunciantes y con ello disminuirían las posibilidades de conocimiento de incumplimientos normativos. Pero la intención real y principal de la norma es que no se vulnere el Derecho de la UE.

- Cuestión prejudicial

No se trata de un recurso directo que se puede plantear ante el TJUE, sino que es algo distinto; se trata de un incidente procesal que surge en el marco de un proceso principal: surge una duda sobre la aplicación o interpretación del derecho comunitario y, el juez nacional, considera que esa duda ha de ser resuelta por el TJUE. Por ello, sólo están legitimados para plantear una cuestión prejudicial los órganos jurisdiccionales de los EM (solo lo puede interponer un Juez o un Tribunal) y por tanto, no existe un acceso directo por parte de los sujetos de derecho europeo puesto que estos no ostentan una legitimación directa.

Si por el contrario surge una duda razonable sobre la aplicación o interpretación del derecho comunitario, tiene que plantear la cuestión. Una cuestión es necesaria cuando la respuesta prejudicial puede condicionar el resultado del litigo nacional o cuando existan dudas razonables acerca de la interpretación o validez de la disposición comunitaria que puede ser aplicada al caso. Si el juez nacional no tiene ninguna duda, no tiene que presentar cuestión prejudicial.

Finalmente mencionar que la sentencia del TJ es vinculante, es decir, son vinculantes para el caso concreto sobre el que se da la interpretación, pero también para cualquier caso futuro en el que se plantee una duda sobre la interpretación o validez del derecho comunitario, en consecuencia, la interpretación hecha en la sentencia por el TJ tiene efectos erga omnes.

3.4 Otros mecanismos de protección del denunciante.

En ocasiones los mecanismos de protección del denunciante no son suficientes y éstos se ven sometidos a procesos penales o civiles muy gravosos para ellos. En apartados anteriores hemos analizado dos sentencias (GUJA y HALET) dictadas en asuntos como estos.

La jurisprudencia del TEDH considera en estos supuestos que prevalece el derecho a la libertad de expresión del denunciante, reconocida en el artículo 10 del Tratado de Roma y los exime de cualquier responsabilidad civil o penal.

Si un denunciante en España ve como la Ley 2/2023 o de la Directiva resultan insuficientes para garantizar su indemnidad, pueden pedir al juez español la aplicación directa del artículo 10 o bien que plantee una cuestión prejudicial, explicada en el punto anterior.

IV. APLICACIÓN PRÁCTICA DE LA LEY 2/2023

4.1En las organizaciones

Una vez analizada la ley desde el punto de visto teórico vamos a analizar la aplicación práctica de la misma en las empresas. Este apartado se ha redactado analizando los diferentes modelos reales a los que se ha tenido acceso en la fase de documentación del trabajo. La Ley no establece un modelo concreto para la implementación del sistema interno de información.

Las empresas obligadas sean públicas o privadas deben a través de su órgano de administración u órgano de gobierno implementar el Sistema interno de información.

Debemos señalar que esta implementación debe hacerse previa consulta con los representantes de los trabajadores. Esta consulta sólo es una consulta, no es necesaria la aprobación por parte de la RLT, ni tampoco negociarlo.

También debe nombrarse a la persona o órgano responsable del canal interno y elegir el instrumento técnico elegido como buzón, que debe cumplir todas las garantías exigidas legalmente.

La implementación pasa por la aprobación por el órgano de administración de la entidad de una **Política del Sistema Interno de Información** en la que se recogen los derechos y garantías que asisten a los informantes y todas las personas afectadas por una comunicación o denuncia y el **Procedimiento de gestión del Sistema Interno de Información** en el que se recogen las normas de gestión de las comunicaciones y denuncias recibidas.

- **Política del sistema interno de información**:

En este instrumento deben concretarse los aspectos siguientes:

- Ámbito de aplicación material y personal, que debe coincidir, como mínimo, con el de la Ley 2/2023
- Principios rectores del sistema: Garantía de acceso a todas las personas, confidencialidad, protección de datos personales, protección del informante y garantía de no represalia, derechos de las personas afectadas por la denuncia i buena fe.
- Medios y forma de presentación de las denuncias, incluidas las denuncias anónimas
- Formas de publicidad de la política (interna y externa)
- Canales externos de denuncia

- **Procedimiento de gestión del Sistema Interno de Información:**

Debe regularse el procedimiento a seguir una vez se recibe una denuncia en el canal, y otros aspectos como la conservación de la documentación y el seguimiento y mantenimiento del canal.

Es de destacar también, con relación a la protección de datos de carácter personal, que la gestión del sistema interno de información debe incorporarse como actividad de tratamiento específica en el Registro de Actividades de Tratamiento de la entidad.

3.2.1 *Análisis de casos prácticos*

Para la elaboración de este trabajo hemos tenido acceso a 3 modelos distintos de implementación del canal:

- Sector público
  - Modelo de decreto de aprobación del sistema interno de información de las entidades del sector público de una Diputación
  - Acuerdo de aprobación de la adaptación del canal de conducta de la empresa XARXA AUDIOVISUAL LOCAL, SL a la nueva 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
- Sector privado
  - Modelo DANONE

Los modelos completos se incorporan a este trabajo como anexos. El primero corresponde al anexo 01 y el segundo corresponde al anexo 02. El modelo Danone es reservado a trabajadores y terceros, por lo que no puede ser adjuntado.

a) **Modelo de decreto de aprobación del sistema interno de información de las entidades del sector público de una Diputación**

En este caso se optó por el modelo siguiente: el órgano de administración de cada entidad dependiente de esta Diputación dicta un Decreto (resolución administrativa) aprobando el sistema interno de información de la entidad.
La Diputación proporciona el modelo para facilitar el trabajo de cada uno de los entes dependiente economizando recursos, y homogeneizar las políticas dentro de su sector público. El modelo se dirige a entes de más de 50 trabajadores.

El decreto incluye:

- **Una política del sistema interno de información** que incorpora los principios siguientes: confidencialidad, garantía en la protección de datos personales, secreto de las comunicaciones, seguridad, exhaustividad, integridad, presunción de inocencia y honor, derecho de audiencia y a la información, colaboración con las autoridades administrativas y judiciales y finalmente, publicidad.

- La instrucción para la implantación y gestión del sistema, donde se regulan la descripción del sistema, ámbito de aplicación, derechos y obligaciones, órganos, responsable del canal, procedimiento de gestión de denuncias, transparencia, publicidad y protección.
- La posibilidad de optar por designar como responsable a una persona física o a un órgano colegiado.

La entidad optó por utilizar la herramienta *Bústia ètica* puesta a disposición del sector público de Cataluña por el consorcio AOC.

La *Bústia Ètica i de Bon Govern* se trata de un dispositivo de participación electrónica concebido en 2017 con el propósito de fortalecer la gestión pública. Su finalidad primordial es proporcionar un foro destinado a reportar acciones u omisiones contrarias al marco legal o a las pautas éticas de comportamiento, siempre y cuando dichos actos tengan relevancia en términos de interés público, entendiéndose aquí contempladas las acciones y omisiones a las que hace referencia los artículos 2 y 3 de la Ley 2/2023.

Esta herramienta se caracteriza por el compromiso en preservar la confidencialidad de la información proporcionada, así como por la opción de permanecer en el anonimato si se desea, tal y como establece obligatoria la norma estudiada. Asimismo, proporciona un entorno seguro para la mantener la comunicación entre el informante y el organismo público correspondiente y permite hacer un seguimiento de la denuncia, aunque se opte por mantener el anonimato. El objetivo principal es crear un ambiente donde se pueda compartir información sin temor a represalias.

No solo garantiza los derechos de los informantes, sino que, además, incorpora herramientas con el fin de garantizar los derechos de la persona acusada.

Finalmente, para evitar el uso inapropiado de la herramienta, como puede ser informar de mala fe o a sabiendas de que la información no es verdadera, se aplican criterios estrictos para el estudio de la información y la *Bústia* está ya preparada para tomar medidas de carácter civil penal o administrativo en estos casos.

b) Acuerdo de aprobación de la adaptación del canal de conducta de la empresa XARXA AUDIOVISUAL LOCAL, SL a la nueva 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 este caso la entidad es una sociedad mercantil de capital público al 100%, por ello el plazo máximo para la implementación del canal era el 13 de junio pese a tener menos de 250 empleados.

Esta entidad ya contaba con un canal de denuncia y un código ético derivado del sistema de prevención de riesgos penales que implementó a raíz de la introducción de la responsabilidad penal de la empresa en el Código penal español.

En este caso el órgano de administración optó por integrar ambos canales de denuncia en uno solo, de acuerdo con el propio espíritu de la Ley, que dice textualmente en su artículo 5. "El Sistema interno de información, en cualquiera de sus fórmulas de gestión, deberá integrar los distintos canales internos de información que pudieran establecerse dentro de la entidad."

La entidad optó por utilizar la herramienta puesta a disposición del sector público de Cataluña por el Consorcio AOC, la *Bústia Ètica,* explicada en el modelo anterior. A través de su canal se puede formular cualquier tipo de denuncia. Esta decisión se tomó para facilitar el acceso al canal de trabajadores y terceros y aumentar su confianza. El denunciante no debe elegir entre distintos buzones internos, solo tiene uno a su disposición.

Finalmente, señalan que tienen un volumen muy bajo de denuncias; al amparo de la ley 2/2023 no han recibido ninguna, y en los años de vigencia del canal (desde 2018) se han recibido únicamente 3 denuncias de temas relacionados con los recursos humanos.

c) Modelo Danone

Danone es una corporación global que opera bajo una estructura empresarial diversificada por zonas geográficas. Es una multinacional especializada en productos lácteos, nutrición y agua embotellada. Se realizó una entrevista con la *compliance officer* a nivel Iberia para que detallara el funcionamiento de su canal interno de denuncias.

Se trata de un canal activo desde 2015, derivado de la responsabilidad penal que se le puede atribuir a las empresas, y que ha sufrido pocas variaciones desde entonces, puesto que ya entonces se adecuaba a lo que la Directiva y la posterior Ley española obliga. Pese a que por confidencialidad no puede revelar qué impacto ha tenido la publicidad y la entrada en vigor de la Ley en cuánto a números de denuncia interpuestos, sí que asegura que es un canal que funciona realmente y que la gente utiliza.

Para publicitar este canal, en la página web a la que tienen acceso todos los empleados y terceros que tengan relación con la empresa tienen un apartado llamado *Danone ethics* donde se explica qué es el canal, cómo funciona, quien es el responsable, cómo se gestionan sus datos y la anonimidad, entre otros aspectos, así como dos vídeos guías para poder efectuar la denuncia.

Existe la posibilidad de aportar las informaciones por escrito o verbalmente, existiendo para ello un servicio de llamadas anónimo. Estas dos formas son completamente confidenciales y, además, existe la posibilidad de que las denuncias se hagan con carácter anónimo. Las denuncias de carácter verbal, además, se pueden hacer al responsable del equipo de *compliance*, pero también a algún miembro del equipo de RRHH o al responsable directo, teniendo estos que guardar la confidencialidad y notificar al equipo responsable de *compliance*. En el caso del canal español, la posibilidad de una cita presencial para denunciar se ofrece a la vez que se manda el acuse de recibo de la denuncia. Esto se hace en un espacio seguro, normalmente fuera de las oficinas, para que no se puedan levantar sospechas.

Al ser un grupo y una compañía mundial, el sistema que usan para la investigación de las denuncias tiene un carácter especial y diferente a los analizados anteriormente. No es un canal específico para denuncias de alguna materia amparada por la Ley 2/2023, sino que abarca una horquilla más grande de temáticas, es decir, este canal integra las denuncias de todo aquello que vaya en contra de la política Danone. Quién recibe la denuncia no es el equipo de *compliance* a nivel España sino que lo hacen sus homólogos a nivel grupo y son ellos mismos quien, en función al tipo de denuncia que es, lo derivan al responsable que, según el caso concreto, crean apto para investigar. Es decir, envían la denuncia a RRHH si es un caso de RRHH o a *compliance* si se trata de una denuncia por ejemplo de corrupción, entre otros y, por otro lado, analizan la adecuación de la persona supuestamente designada para el estudio del caso. Para ello, analizan los posibles conflictos de intereses que pudiese tener e intentan, por ejemplo, que un mismo equipo no se investigue entre sí, por posibles interferencias que pudieran existir.

Hay casos en los que la información que se da no es suficiente para poder llevar a cabo una investigación, como por ejemplo si alguien denunciase algo como “hay un jefe que acosa a sus empleados”. En caso de que la denuncia no fuese anónima, el encargado de la investigación hablaría con el informante para recabar más información, como quién es ese jefe o qué entiende por acoso. Las denuncias anónimas, sin embargo, se tratan de manera un poco distinta. En el momento en el que una persona decide informar de manera anónima, se le envía, junto con el acuse de recibo, un código de referencia de la denuncia. Este código sirve para entrar en la propia web del canal y ver las actualizaciones que hay sobre el caso, así como para poderse comunicar con el investigador de forma anónima y que éste pueda solicitar más información. Es la única forma que tiene el denunciante y la persona responsable del canal de comunicación en caso de denuncia anónima.

De la misma manera, será el equipo de *compliance* a nivel Iberia el que deberá garantizar que el informante no tenga ningún tipo de represalia siempre que la denuncia sea de buena fe. En caso de que la denuncia sea de mala fe, se perseguirá al denunciante.

4.2 *Oficina Antifrau* de Cataluña en el papel de Canal Externo

La *Oficina Antifrau de Cataluña* tiene el papel de Autoridad Independiente desde el pasado 10 de marzo, cuando el Parlemento catalán le otorgó las competencias.

Como se ha comentado en apartados anteriores, tiene una serie de funciones.

Tras una entrevista con la *Cap de Relacions institucionals, Visibilitat i Participació* de la propia oficina, se destacan los siguientes puntos.
La Oficina Antifraude cumple varias funciones importantes. En primer lugar, se encarga de gestionar los canales internos, como el registro de denuncias. Además, posee la capacidad de imponer sanciones, lo cual es crucial. También desempeña un papel en la promoción de una cultura de informar y alertar sobre irregularidades, fomentando un ambiente donde las personas pueden informar sin temor a represalias. Esto se logra mediante herramientas como códigos éticos en las empresas, que deberían prohibir tanto represalias como prácticas que puedan revelar la identidad del denunciante. Los códigos éticos no son la única forma de fomentar las denuncias, existen otras, como la formación.

Es evidente que lo que se busca es concienciar a todos los empleados de que utilizar el canal interno de denuncia no es un acto desleal hacia la empresa, sino todo lo contrario. Se trata de algo positivo y respaldado por una serie de derechos como denunciante, ya que se está llevando a cabo un acto cívico en beneficio de la protección del interés público.

El interés público no solo es respaldado por las instituciones públicas, sino también por las empresas privadas cuando actúan de manera responsable. La responsabilidad de las empresas va más allá de simplemente tener un departamento de Responsabilidad Social Corporativa (RSC). Se trata de comprender la responsabilidad de las empresas en términos de transparencia, gestión de la información y asumir la responsabilidad de sus propias acciones. Esto incluye la noción de "huella social", es decir, el conjunto de impactos, tanto positivos como negativos, que una empresa tiene en el medio ambiente, la inclusión y otros aspectos sociales.

La Oficina Antifrau juega un papel de *crupier*, en el que su función es investigar si la denuncia que les llega es verosímil y, por otro lado, velarán por que el informante no sufra represalias. Pero no son ellos los que llevarán la investigación de todas las materias ya que, en algún caso, como puede ser Seguridad nuclear, no tienen una formación suficiente como para poder juzgar sobre el tema.

Para que esta obligación se pueda llevar a cabo, las empresas tienen la obligación de colaborar con el organismo, aunque, a diferencia de lo que ocurre con otras oficinas, la *Oficina Antifrau* no tenía hasta ahora el poder sancionador.

La actual facultad sancionadora se encuentra en los términos de la Ley 2/2023. Es decir, tienen autoridad para sancionar lo establecido en la Ley 2/2023. Por lo tanto, la negativa de colaboración por parte de la empresa no sería objeto de sanción, a menos que pueda relacionarse con lo establecido en la Ley 2/2023, como por ejemplo si estuvieran tomando represalias contra algún denunciante trabajador.

En otros casos, como si por ejemplo un ente como un Ayuntamiento no colabora, ese hecho deberá quedar registrado en el informe anual y solo se podrá ejercer si se puede relacionar con aquello establecido en la Ley 2/2023.

4.3 Reflexiones sobre la aplicación

- *Cuestiones controvertidas con relación a la aplicación de la ley 2/2023*

La aplicación de la Ley 2/2023 genera distintas cuestiones controvertidas que deberán resolverse en algún momento. Algunas de ellas son de fondo como por ejemplo es la todavía deficiente protección del informante frente a, por ejemplo, acciones penales. Bien es cierto que finalmente ante una reclamación ante el TEDH el denunciante probablemente verá reconocida su condición y restablecidos sus derechos, pero ello le obliga a un costoso periplo judicial, no siempre al alcance de todo el mundo.

Vamos a centrarnos solo en las cuestiones controvertidas desde el punto de vista de la empresa.

- *Exceso de obligaciones formales para las empresas*

Como ya he dicho al principio de este trabajo las empresas, tanto públicas como privadas, están sometidas a una infinidad de obligaciones formales, más allá de las estrictamente fiscales o laborales. La mayoría de estas obligaciones deriva de la normativa comunitaria. La tradición normativa española (y cultural) se basa en la sanción. Se impone una obligación y se añade una sanción por el incumplimiento. Sin sanción es difícil hacer cumplir una norma.

La normativa europea, en cambio, tiende a la cultura del cumplimiento; la normativa impone una serie de criterios que deben cumplirse, si no se cumplen no hay una sanción directa, pero si ocurre algo, la empresa es responsable por el incumplimiento; en cambio si es capaz de demostrar que ha implementado todos los controles o medidas legales necesarias queda eximido de responsabilidad. Ocurre así con la responsabilidad penal de

las empresas o con el cumplimiento de la normativa relativa a la protección de datos personales.

Estas obligaciones se extienden a todo tipo de empresas, suelen ser más exigentes a partir de una horquilla que va entre los 50 y los 250 trabajadores, pero las obligaciones son comunes a todas.

Generalizando, el cumplimiento consiste en implementar un código de conducta o normativa interna, a menudo consensuada con los representantes de los trabajadores, implementación de controles, mecanismos de denuncia y formación al personal, colaboradores, proveedores, etc. Los controles son normalmente internos, lo que genera problemas de independencia, punto que analizaré más adelante.

¿Qué ocurre en la práctica? Cada novedad normativa en materia de cumplimiento obliga a contratar un asesor externo para implementar la norma, y seguir todos los pasos detallados en el párrafo anterior.

Esto provoca la situación siguiente:

Muchas empresas tienen actualmente los instrumentos internos siguientes derivados de las diferentes leyes:

- Código de conducta o código ético de prevención de riesgos penales
- Plan de medidas antifraude, si gestiona fondos de la UE
- Sistema interno de información derivado de la ley 2/2023
- Normativa interna de protección de datos personales
- Normativa interna en materia de seguridad de la información
- Plan de igualdad
- Normativa de prevención del acoso en el trabajo

Con el agravante que, a veces, las normas se solapan y se contradicen entre ellas.

De cada una de ellas deriva un órgano responsable del control (comité de seguridad, de conducta, etc.), a menudo un canal de denuncia exclusivo, y finalmente, una formación al personal. Estos órganos de control están compuestos por diferentes integrantes de la empresa, pero se suele dar el caso en organizaciones no muy grandes que siempre son las mismas personas: gerencia, responsable de recursos humanos y asesor jurídico interno, si lo hay.

La situación es grave ya que, al final, directivos y trabajadores se pierden en códigos y normas que, en lugar de ayudarles en la gestión, les complican la gestión diaria, les cargan con controles excesivos y pierden la utilidad que debieran tener. Además de los recursos materiales y personales destinados a ello.

Esta situación es fruto del exceso de obligaciones y de la dispersión normativa. La solución pasa por tener una visión global de todas las obligaciones e intentar integrar en elementos normativos únicos y órganos de control únicos todos los procesos. De este modo las empresas podrían optimizar las herramientas y hacerlas realmente efectivas para la organización.

Artículo 5.2 d) Integrar los distintos canales internos de información que pudieran establecerse dentro de la entidad.

- *Falta de independencia de los órganos internos de control*

La Ley 2/2023 obliga a que las empresas tengan una persona o un órgano Responsable del sistema interno de información. Tal como dice la propia norma en el artículo 8, *el Responsable del Sistema deberá desarrollar sus funciones de forma independiente y autónoma respecto del resto de los órganos de la entidad u organismo, no podrá recibir instrucciones de ningún tipo en su ejercicio, y deberá disponer de todos los medios personales y materiales necesarios para llevarlas a cabo.* Además *en el caso del sector privado, el Responsable del Sistema persona física o la entidad en quien el órgano colegiado responsable haya delegado sus funciones, será un directivo de la entidad, que ejercerá su cargo con independencia del órgano de administración o de gobierno de la misma. Cuando la naturaleza o la dimensión de las actividades de la entidad no justifiquen o permitan la existencia de un directivo Responsable del Sistema, será posible el desempeño ordinario de las funciones del puesto o cargo con las de Responsable del Sistema, tratando en todo caso de evitar posibles situaciones de conflicto de interés.*

Resulta tremendamente difícil que ante una situación realmente grave un directivo (que no deja de ser un trabajador en muchas ocasiones) pueda resolver una situación en contra de los intereses de la empresa, por temor a las represalias o consecuencias negativas que el asunto pueda acarrearle a sí mismo.

En otros casos en organizaciones no muy grandes donde las estructuras gerenciales y directivas están compuestas por pocas personas es muy probable que los denunciados sean los propios Responsables o miembros del órgano responsable, con lo que el canal interno devendrá ineficaz necesariamente.

Claro que siempre quedan los canales externos a disposición de los denunciantes, pero eso les resulta más gravoso.

Eso mismo ocurre en las entidades del sector público. Sería mejor que en estos casos que el canal interno estuviera en su entidad matriz (diputación, ayuntamiento, etc…) que no en la propia organización para garantizar el éxito del canal. Las organizaciones muchas veces son de tan poco tamaño que muchas veces el denunciado puede ser el responsable de gestionar el canal.

V. CONCLUSIONES

El impulso de la ética corporativa y la lucha contra la corrupción ha cobrado en los últimos 25 años vital importancia en nuestra sociedad. La Convención de Naciones Unidas contra la corrupción del 31 de octubre de 2003, la Directiva 2019/1937, relativa a la protección de las personas que informen sobre infracciones de derecho de la Unión Europea, y finalmente la 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, conforman el sistema legal español relativa a la protección de las personas alteradoras de corrupción.

La Ley 2/2023 obliga a empresas y sector público a adoptar una serie de medidas para dotarse de un canal interno de denuncia de forma obligatoria, previendo también un sistema sancionador para las organizaciones que lo incumplan. La Ley prevé también la existencia de un canal externo e incluso la posibilidad de revelación pública de la información en algunos casos.

A pesar de ello, existen algunos supuestos en que la protección al denunciante prevista legalmente, es insuficiente y los denunciantes se ven sometidos a una persecución judicial gravosa que acaba en ocasiones en sanciones penales. Para estos supuestos cabe la invocación ante el Tribunal Europeo de Derechos Humanos del derecho a la libertad de expresión artículo 10 del Convenio de Roma.

Las empresas españolas afectadas por la obligación de poner en marcha el canal interno de denuncia en el mes de junio de 2023 lo han hecho mayoritariamente ante el miedo a recibir una sanción. Los modelos seguidos son bastante homogéneos.

Finalmente, se pone de manifiesto un exceso de reglamentación de la actividad empresarial relacionado con el cumplimiento normativo. Esto provoca que las empresas se doten de los instrumentos obligatorios, como el canal interno de denuncia, con el único objeto de cumplir la norma y evitar la sanción, cuando lo conveniente sería que las empresas tuvieran una visión global en cuanto al cumplimiento normativo, integrando los diferentes mecanismos e instrumentos que afectan a su regulación interna y su cultura corporativa. Así los códigos éticos se integran efectivamente en las organizaciones y devienen instrumentos eficaces valorados interna y externamente.

VI. BIBLIOGRAFÍA

- Alcacer, R. (2023). Expansión. https://www.expansion.com/juridico/opinion/2023/04/13/64382365e5fdea951b8b45da.html
- Administració Oberta de Cataluña. https://www.aoc.cat/blog/2021/bustia-etica-10-idees-per-entendre-la/
- Administració Oberta de Cataluña. https://www.aoc.cat/serveis-aoc/bustia-etica/
- Crónica de Jurisprudencia. (2008). https://repositorio.gobiernolocal.es/xmlui/bitstream/handle/10873/403/qdl18_14_jur02_tedh.pdf?sequence=1&isAllowed=y
- Directiva (UE) N°2019/1937 del Parlamento Europeo, de 23 octubre de 2019, relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión. (DOUE L [en línea], núm. 305, de 26 de noviembre de 2019, páginas 17 a 56). <https://www.boe.es/doue/2019/305/L00017-00056.pdf> [Consulta: 2 de marzo de 2023]
- España. 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. (BOE [en línea], núm. 44, de 21 de febrero de 2023). <https://www.boe.es/buscar/act.php?id=BOE-A-2023-4513> [Consulta: 2 de marzo de 2023]
- Escura. https://www.escura.com/es/canal-de-denuncias-nueva-ley/
- European Comission. Directorate General for Justice and Consumers: Frequently Asked Ques- tions. 23 de abril de 2018. Explanatory memorandum of the Proposal for a Direc- tive of the European Parliament and of the Council on the protection of persons reporting on breaches of Union Law ("Exposición de motivos de la Propuesta de Directiva del Parlamento Europeo y del Consejo sobre la protección de personas que informan sobre la infracción del Derecho de la Unión"). Financial Incentives for Whistleblowers, informe de la Financial Conduct Authority y de la Prudential Regutlation Authority del Reino Unido, de julio de 2014. https://www.fca.org.uk/publication/ financial-incentives-for-whistleblowers.pdf
- García Mª Ángeles. (2023). Caxlandia. https://www.politicafiscal.es/equipo/maria-angeles-garcia-frias/proteccion-whistle-blower-tedh-12-febrero-23
- González, V. (2023). Confilegal. https://confilegal.com/20230215-el-tedh-condena-a-luxemburgo-a-pagar-55-000-euros-a-uno-de-los-informantes-del-caso-luxleaks/
- Hay derecho. (2021). https://www.hayderecho.com/2021/12/19/la-directiva-comunitaria-1937-2019-sobre-proteccion-del-denunciante-de-corrupcion-las-infracciones-verbales/
- Le Monde with AFP, Hungary strips 'anti-LGBTQ' section from whistleblower law.(Mayo2023).https://www.lemonde.fr/en/hungary/article/2023/05/23/hungary-strips-anti-lgbtq-section-from-whistleblower-law_6027758_220.html
- López Cumbre, L.: "Protección para los trabajadores denunciantes (whistleblowers)", Análisis GA_P. (2019). https://www. ga-p.com/wp-content/uploads/2019/12/Protección- para-los-trabajadores-denunciantes-whistle- blowers.-1.pdf

- Martínez Saldaña, D., Abril Martínez, J., Rodríguez Celada, E., Reyes Rico, L. (2019). La protección del *Whistleblower* tras la directiva (UE) 2019/1937. análisis del nuevo marco jurídico desde la perspectiva del derecho laboral, público, penal y de protección de datos. *Actualidad Jurídica Uría Menéndez.* https://www.uria.com/documentos/publicaciones/6845/documento/art02.pdf?id=9331&forceDownload=true
- MIRANZO DÍAZ, J. "La nueva Directiva europea de protección del denunciante: un análisis desde el derecho público" *Revista General de Derecho Europeo*, 49, 2019. https://www.obcp.es/opiniones/la-nueva-ley-22023-de-proteccion-del-informante
- Molins. (2023). https://www.molins.eu/breve-resumen-sentencia-halet-c-luxemburgo/
- Morcillo, N. (2023). Cinco Días. https://cincodias.elpais.com/companias/2023-02-15/bruselas-lleva-a-espana-ante-el-tjue-por-incumplir-la-directiva-sobre-la-proteccion-al-denunciante.html
- Sentencia del Tribunal Europeo de Derechos Humanos, 12 de febrero del 2008, N°14277/04, Caso Guja vs. Moldavia
- Sentencia del Tribunal Europeo de Derechos Humanos, 14 de febrero del 2023, N°21884/18, Caso LuxLeaks, Halet vs. Luxemburgo
- Oficina Antifraude Cataluña. (2018). https://www.antifrau.cat/ca/llei-2-2023-20-febrer-reguladora-proteccio-persones-informin-infraccions-normatives-lluita-contra-corrupcio-algunes-reflexions-molts-dubtes
- Wolters Kluwer. (2023). https://www.wolterskluwer.com/es-es/expert-insights/directiva-whistleblowing-para-canal-denuncias
- Venezuela, F. (22 de junio de 2023). *Factorial*. https://factorialhr.es/blog/directiva-whistleblower/

VII. ANEXOS

7.1 Anexo 01

DECRET

Aprovar el sistema intern d'informació de l'entitat del sector públic de la Diputació de ... XXXXXXXXX

(expedient 2023/xxxx)

Antecedents

1. La Directiva (UE) 2019/1937 del Parlament Europeu i del Consell de 23 d'octubre (en endavant Directiva 2019/1937), amb la finalitat de reforçar l'aplicació del Dret i les polítiques de la Unió Europea mitjançant l'establiment d'unes normes mínimes comunes que proporcionin un nivell de protecció a les persones que informin sobre infraccions del Dret de la Unió, obliga a les entitats jurídiques del sector públic i privat a establir canals i procediments de denúncia interna i de seguiment.

2. La Llei 2/2023, de 20 de febrer, reguladora de la protecció de les persones que informin sobre infraccions normatives i de lluita contra la corrupció (en endavant Llei 2/2023) transposa la Directiva (UE) 2019/1937 a l'ordenament espanyol. La Llei obliga als ens dels sector públic i del sector privat a la implantació d'un Sistema intern d'informació que permeti a les persones que en un context laboral o professional detectin infraccions penals o administratives greus o molt greus, posar-les en coneixement mitjançant els mecanismes que s'hi regula. La finalitat de la norma és la de protegir a aquestes persones que informin, específicament, sobre infraccions del Dret de la Unió previstes a l'esmentada Directiva (UE) 2019/1937 i infraccions penals i administratives greus i molt greus de l'ordenament jurídic intern.

3. Aquesta regulació del dret estatal compta amb antecedents, com ho són l'article 24.1 de la Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals, en referència a les entitats de dret privat. Així com el Reial decret llei 11/2018, del 31 d'agost, que va introduir a la Llei 10/2010, del 28 d'abril, de prevenció del blanqueig de capitals i del finançament del terrorisme. En coherència amb aquest context, la Llei 2/2023 preveu la presentació de denúncies anònimes i obliga, en tot cas i de conformitat amb la Directiva (UE) 2019/1937, a la protecció de l'informant i a la preservació de la seva confidencialitat.

4. En quant a l'obligatorietat de disposar del Sistema intern d'informació que prescriu la Llei 2/2023, el seu article 13 disposa que totes les entitats que integren el sector públic, sense excepció, estan obligades a disposar de Sistema intern d'informació. És el cas de les entitats pertanyents al sector públic amb personalitat jurídica pròpia vinculades o dependents que tinguin 50 treballadors o més.

5. Aquests ens del sector públic dependents i vinculats de la Diputació de ... de 50 treballadors o més, de conformitat amb la mateixa Llei 2/2023, han d'adoptar els seu propi Sistema intern d'informació, dotar-lo de recursos per a les investigacions i

tramitacions i designar el seu responsable. La Diputació facilitarà assistència a aquests ens del seu sector públic que ho puguin necessitar.

6. (...)

7. D'acord amb el context corporatiu i comptant actualment amb un marc legal estatal que prescriu l'obligatorietat de d'establir el Sistema intern d'informació, l'entitat XXXXXXX ha impulsat diverses accions per dotar-se dels requeriments mínims legalment previstos i per a la posada en funcionament del Sistema dins del termini establert en l'esmentada disposició transitòria segona de la Llei 2/2023, això és, en el termini de tres mesos a comptar des de l'entrada en vigor de la Llei el passat 13 de març, termini que s'exhaureix el proper 13 de juny.

8. Entre les anteriors accions, en primer terme, s'ha elaborat una minuta d'Instrucció d'implantació del Sistema intern d'Informació a la entitat XXXXXXXXXXX, de forma anàloga i adaptada a l'elaborada a la Diputació de ... i ens del seu sector públic de menys de 50 treballadors.

   L'esmentada minuta que es proposa a aprovació va ser sotmesa al tràmit de prèvia consulta amb la representació legal de les persones treballadores en data 99999999.

9. En segon terme, s'ha treballat en determinar quina ha de ser l'eina tecnològica que permeti la presentació d'informacions al Sistema, és dir el canal intern d'informació, previst als articles 5 i 7 de la Llei 2/2023. Aquests treballs s'han emmarcat en la col·laboració que la Diputació té establerta amb la Xarxa de Governs Oberts (XGO) i, en el si d'aquesta, amb el Consorci Administració Oberta de Catalunya (Consorci AOC), a qui s'ha sol·licitat l'alta en el Servei de "Bústia ètica" que permet l'establiment del canal per informar d'infraccions normatives complint amb els requisits legals i emprant el programari de codi obert Globaleaks, integrat en el catàleg de serveis del Consorci AOC.

   Així mateix, aquest Servei "Bústia ètica" permet l'elaboració del formulari per a la presentació de les comunicacions o alertes que poden ser també anònimes, de conformitat amb el previst a la Llei 2/2023.

10. En tercer lloc, s'ha treballat en l'elaboració d'una política o estratègia que enuncia els principis generals del Sistema intern d'informació d'acord amb l'establert a l'article 5.2.h) de la Llei 2/2023, la qual es proposa a aprovació i haurà de ser degudament publicitada internament a l'entitat XXXXXXX.

11. Així mateix, i en compliment del disposat a l'article 25 de la Llei 2/2023, es preveu proporcionar informació de manera clara i accessible sobre l'ús del canal intern a la pàgina web de l'entitat, així com dels principis essencials que preveu la Instrucció per a la implantació i gestió del sistema Intern d'Informació de l'entitat XXXX que es proposa a aprovació.

Fonaments de dret

La normativa específica en la que es fonamenta jurídicament aquesta resolució està constituïda per:

1. La Directiva (UE) 2019/1937 del Parlament Europeu i del Consell, de 23 d'octubre, relativa a la protecció de les persones que informin sobre infraccions del Dret de la Unió, estableix l'obligació als Estats membres de transposar la norma al Dret nacional.

2. La Llei 2/2023, de 20 de febrer, reguladora de la protecció de les persones que informin sobre infraccions normatives i de lluita contra la corrupció, que transposa a l'ordenament jurídic espanyol la Directiva (UE) 2019/1937 del Parlament Europeu i del Consell.

3. En concordança amb l'establert al títol VI de l'esmentada Llei 2/2023, és d'aplicació la Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals que, entre d'altres, transposa al dret estatal el Reglament (UE) 2016/679 del Parlament Europeu i del Consell, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques pel que fa al tractament de les dades personals.

4. En compliment de la DA 7a de la Llei 3/2023, de 16 de març, de mesures fiscals, financeres, administratives i del sector públic per al 2023, s'ha de donar trasllat a l'Oficina Antifrau de Catalunya de la present resolució, atesa la seva condició d'Autoritat Administrativa Independent (AAI).

L'adopció d'aquesta resolució es justifica en la circumstància d'haver de donar compliment al termini previst a la disposició transitòria segona de la Llei 2/2023 que s'exhaureix el proper 13 de juny de 2023, raó per la qual la seva tramitació no es pot ajornar sense que se'n derivi un perjudici rellevant per a l'interès públic que impulsa l'actuació de la entitat.

L'adopció d'aquesta resolució correspon a_____, d'acord amb l'article ___ dels Estatuts de l'entitat

En virtut de tot això, es proposa l'adopció de la següent

RESOLUCIÓ

Primer. APROVAR la implantació del Sistema intern d'informació a l'entitat XXXXXXXXXX.

Segon. APROVAR la "Política estratègica del Sistema intern d'informació de l'entiitat XXXXXXX", que anuncia els principis generals que inspiren el Sistema, d'acord amb el text que s'adjunta com a l'Annex I d'aquesta resolució.

Tercer. APROVAR la "Instrucció per a la implantació i gestió del Sistema intern d'informació de l'entitat XXXXXXXXXX" d'acord amb el text que s'adjunta com a l'Annex II d'aquesta resolució.

Quart. DISPOSAR que la presentació de les informacions a què es refereix aquesta resolució s'haurà de vehicular a través de l'eina subministrada pel Consorci AOC disponible en el seu catàleg de serveis.

Cinquè. FER DIFUSIÓ de la Instrucció per a la implantació i gestió del Sistema intern d'informació i de la Política estratègica del Sistema intern d'informació de l'entitat XXXXXXXXXX que s'aproven amb la present resolució.

Sisè. ESTABLIR l'obligatorietat d'observança de la Instrucció per a la implantació i gestió del Sistema intern d'informació per part de tots els òrgans i/o centres gestors de l'entitat XXXXXXXXX.

Setè. DONAR TRASLLAT a l'Oficina Antifrau de Catalunya (AAI) de la present resolució.

Vuitè. DONAR COMPTE a *òrgan col.legiat plenari de l'entitat*

ANNEX I al Decret d'aprovació el sistema intern d'informació de l'entitat XXXXXXXX

POLÍTICA DEL SISTEMA INTERN D'INFORMACIÓ DE L'ENTITAT XXXXXXXXXXXX

Per acord del ple la Diputació de ... va aprovar el Sistema d'Integritat Institucional i el Pla de Mesures Antifrau. El Sistema d'integritat institucional és l'element estructural d'integritat corporativa de la Diputació de ..., incorpora els instruments en matèria d'infraestructura ètica i bon govern, que el Pla estructura entorn del cicle antifrau (prevenció, detecció, correcció i persecució).

El Pla de Mesures Antifrau és el principal element que integra el Sistema d'Integritat Institucional de la Diputació. Mitjançant el Pla de Mesures Antifrau es despleguen les accions concretes per al control del risc de frau en el sí de la Diputació de ... i els ens del seu sector públic que s'hi puguin adherir. De conformitat amb la normativa que el regula, és objecte de revisió anual o bianual, espacialment pel que fa referència a l'avaluació del risc de frau. Per aquest motiu, el ple corporatiu en acord, va donar compte del balanç de l'execució del Pla de Mesures Antifrau vigent i es va aprovar l'actualització del Sistema d'Integritat Institucional i el Pla de Mesures Antifrau de la Diputació de ... i dels ens del seu sector públic.

Aquestes accions permeten donar resposta a l'obligació legal d'implementar un Sistema intern d'Informació, que prescriu la Llei 2/2023 de 20 de febrer, reguladora de la protecció de les persones que informin sobre infraccions normatives i de lluita contra la corrupció (en endavant Llei 2/2023), que transposa a l'ordenament espanyol la Directiva (UE) 2019/1937 del Parlament Europeu i del Consell, de 23 d'octubre, relativa a la protecció de les persones que informin sobre infraccions del Dret de la Unió.

La Llei 2/2023, a més d'exigir a totes les administracions públiques la posada en funcionament de canals segurs d'alerta d'infraccions normatives, estableix un seguit de requisits i condicions materials i formals com l'establiment dels canals d'alerta, el règim de protecció de les persones informants i la publicitat del sistema, entre altres.

Així mateix, l'article 5.2 apartat h) de la Llei 2/2023 obliga a les administracions, organismes, empreses i demés entitats obligades, a comptar amb una política o estratègia que enunciï els principis generals del Sistema intern d'informació i de la defensa de l'informant.

Per aquest motiu, a continuació s'enuncien els principis generals que inspiren el Sistema intern d'informació de l'entitat XXXXXXX:

Confidencialitat
Garantia en la protecció de dades personals
Secret de les comunicacions
Seguretat
Exhaustivitat
Integritat
Presumpció d'innocència i honor
Dret d'audiència i a la informació
Col·laboració amb les autoritats administratives i judicials
Publicitat

1. Confidencialitat

- Es garanteix la confidencialitat de l'informant, dels tercers mencionats en la comunicació, així com durant el procés d'avaluació i en les actuacions que es desenvolupin en la gestió i tramitació de la informació.

2. Garantia en la protecció de dades personals

- S'impedirà l'accés de personal no autoritzat a la informació que es comuniqui.

- Participació del Delegat de Protecció de Dades personals com a garantia d'adequació de les actuacions del Responsable del Sistema a la normativa vigent en matèria de protecció de dades personals.

3. Secret de les comunicacions

- Es mantindrà del secret respecte de qualsevol aspecte relacionat amb la informació comunicada.

- Es garanteix el tracte confidencial de la persona que presenti anònimament la seva comunicació.

4. Seguretat

- Es disposarà d'un canal d'accés independent i segur que permeti informar infraccions normatives.

- Es garanteix la conservació adient de la informació i la documentació que es faciliti a través del canal intern habilitat a l'efecte.

5. Exhaustivitat

- Investigació exhaustiva de les informacions rebudes, podent sol·licitar més dades per esclarir els fets.

- L'aportació d'al·legacions i/o mitjans de prova per part de l'informant i dels tercers mencionats en la comunicació serviran per a la fonamentació de la proposta de resolució i la resolució de l'expedient.

6. Integritat

- Seguiment i avaluació continuada dels instruments d'integritat de la Diputació de ... en foment de la cultura de la transparència i informació com a mecanismes d'integritat per a la prevenció i detecció d'amenaces a l'interès públic, així com la posterior correcció, si s'escau.

7. Presumpció d'innocència i honor

- Es garanteix el respecte a la presumpció d'innocència i a l'honor de les persones afectades per les comunicacions facilitades mitjançant el canal intern d'informació.

8. Dret d'audiència i d'informació

- Les persones afectades seran escoltades i podran presentar al·legacions en el format que considerin en qualsevol moment de la instrucció.

- Es permetrà l'accés a l'expedient que s'incoï arran de la comunicació a les persones afectades pel mateix.

- S'estableix la possibilitat de comparèixer a l'expedient amb assistència lletrada.

9. Col·laboració amb les autoritats administratives i judicials

- Col·laboració amb l'Autoritat Independent de Protecció de l'Informant, amb l'autoritat o òrgan competent de Catalunya i amb altres autoritats administratives competents.

- Remissió al Ministeri Fiscal de les informacions que indiquin fets constitutius de delicte, o a la Fiscalia Europea o altre organisme competent, si fos el cas.

10. Formació i difusió

- Compromís corporatiu en la implantació de la cultura de la integritat en l'actuació pública

- Facilitar la formació necessària a tots els empleats corporatius en la detecció dels indicis de manca d'integritat en l'actuació administrativa.

- Promoure la implicació activa dels empleats corporatius en la vigilància contra conductes constitutives d'actuacions il·lícites en l'actuació administrativa.

- Publicació de forma clara, i fàcilment accessible, d'informació sobre el Sistema intern d'informació de l'entitat i dels principis essencials del procediment de gestió.

- Màxima difusió i informació per a coneixement del personal que presta servei a l'entitat, així com de tots aquells tercers que estan o han estat vinculats o relacionats amb la mateixa.

ANNEX II al Decret d'aprovació el sistema intern d'informació de l'entitat XXXXXXX

INSTRUCCIÓ PER A LA IMPLANTACIÓ I GESTIÓ DEL SISTEMA INTERN D'INFORMACIÓ DE L'ENTITAT XXXXXXXX.

ANTECEDENTS

La Convenció de Nacions Unides contra la corrupció del 31 d'octubre del 2003, ratificada per Espanya el 9 de juny del 2006 indica que els ens públics han d'establir mecanismes i sistemes que facilitin que els servidors públics denunciïn qualsevol acte de corrupció a les autoritats competents, quan en tinguin coneixement en l'exercici de les seves funcions. També regula la necessitat de protegir les persones que, en compliment del seu deure ciutadà, denunciïn casos de frau o corrupció, tot assegurant-ne la indemnitat. Es preveu també la necessitat de disposar i oferir bases de coneixement, formació i sensibilització, capaces de crear una cultura de rebuig de tota conducta que propiciï la corrupció. Concretament, l'article 5 de la Convenció, preveu l'obligació de formular i aplicar polítiques contra la corrupció que promoguin la participació de la societat i reflecteixin els principis de l'imperi de la llei, la gestió adequada dels assumptes i béns públics, la integritat, la transparència i l'obligació de retre comptes.

La Directiva (UE) 2019/1937 del Parlament Europeu i del Consell, del 23 d'octubre, relativa a la protecció de les persones que informin sobre infraccions del Dret de la Unió va introduir a l'ordenament jurídic comunitari un seguit d'obligacions relatives a la implantació de canals interns i externs de comunicació de conductes il·legals, antijurídiques o irregulars. El termini per a la transposició d'aquesta Directiva finalitzava el desembre de 2021, data a partir de la qual se'n podia invocar l'efecte directe.

L'Estat espanyol en transposició de l'esmentada Directiva, va aprovar la Llei 2/2023, de 20 de febrer, reguladora de la protecció de les persones que informin sobre infraccions normatives i de lluita contra la corrupció (en endavant Llei 2/2023), que va entrar en vigor el passat 13 de març. La finalitat de la Llei és atorgar protecció davant de les represàlies que puguin patir les persones físiques que informin sobre accions o omissions incloses en seu àmbit material d'aplicació. La Llei regula, com a mecanisme preferent per informar d'aquelles infraccions, el Sistema Intern d'Informació el qual ha de complir determinats requisits i es preveu com a obligatori per a totes les entitats que integren el sector públic, d'acord amb l'article 13 de la mateixa Llei.

Amb aquesta Instrucció s'implanta el Sistema Intern d'informació de l'entitat XXXXXXXXX, per tal que les persones amb legitimació subjectiva, objectiva i material atorgada per la Llei 2/2023 que en vulguin fer ús comptin amb un sistema de funcionament clar, confidencial i segur[6].

[6] Els termes denúncia, denunciar, denunciant i altres termes relacionats amb el mot denúncia que s'esmenten en aquest Protocol s'han d'entendre en el sentit que especifica l'article 5 de la Directiva (UE) 2019/1937 i en equiparació als conceptes informació d'infraccions normatives, informants i altres concordants, que regula a la Llei 2/2023.

Des del punt de vista objectiu, la Instrucció que s'aprova no té caràcter normatiu, en no innovar l'ordenament jurídic. Té el caràcter d'acte general d'execució de la Llei 2/2023, en procedir a la implantació del Sistema Intern d'Informació (SIDI) a l'entitat XXXXXXXXX, en compliment del que la dita llei estableix (art. 5.1).

ÍNDEX

CAPÍTOL I. EL SISTEMA INTERN D'INFORMACIÓ. DRETS I OBLIGACIONS DE PERSONES INFORMANTS I PERSONES AFECTADES

Article 1. Objecte de la Instrucció

L'objecte d'aquesta Instrucció és la regulació de la implantació i el procediment de gestió del Sistema Intern d'informació (en endavant, SIDI) de l'entitat XXXXXXXXXX, en el marc i en compliment de la Llei 2/2023, de 20 de febrer, reguladora de la protecció de les persones que informin sobre infraccions normatives i de lluita contra la corrupció (en endavant Llei 2/2023).

Article 2. Finalitat del Sistema Intern d'informació

1. El SIDI es constitueix com a instrument d'integritat de l'entitat per tal de donar compliment a la Llei 2/2023 i que les persones informants incloses al seu àmbit subjectiu, objectiu i material d'aplicació comptin amb un sistema clar, confidencial i segur per informar de les infraccions normatives previstes a l'esmentada norma i gaudir de la protecció que regula la Llei.

   El SIDI és el mecanisme preferent per a la posada en coneixement d'alertes consistents en informar d'accions o omissions que puguin constituir infraccions normatives, en els termes de l'article 3 de la Llei 2/2023, del 20 de febrer i de la Directiva (UE) 2019/1937, del 23 d'octubre.

2. El SIDI garanteix el tracte confidencial i segur a totes les comunicacions que es rebin a través del seu Canal Intern d'Informació (en endavant, Canal), tant respecte de la persona informant com de les actuacions de tramitació i investigació, dels fets comunicats i de la persona o persones a les quals es faci referència. Així mateix, garanteix el tracte confidencial a la persona informant que així presenti la seva comunicació anònimament.
   Es prestarà la protecció de l'informant que preveu la Llei 2/2023, a les persones incloses en el seu àmbit subjectiu, i en referència al seu àmbit objectiu i material d'aplicació.

Article 3. Elements del Sistema Intern d'informació

El SIDI de l'entitat XXXXXXXXX comprèn el següents elements:

a) Canal d'accés, independent per a cadascuna de les entitats, confidencial i segur (el Canal)
b) Responsable del Sistema Intern d'Informació i unitat de suport (RSIDI)
c) Política i estratègia del SIDI
d) Procediment de gestió de les informacions rebudes i les garanties per a la protecció dels informants.

Article 4. Àmbit objectiu d'aplicació del Sistema Intern d'informació

El SIDI de l'entitat XXXXXX adopta com a pròpia, amb les adaptacions adients, la Instrucció que implanta i desenvolupa el SIDI de la Diputació de ... i les seves entitats del seu sector públic amb menys de 50 treballadors, llevat la designació del Responsable del Sistema Intern d'Informació que serà propi de l'entitat XXXXXXX.

Article 5. Àmbit subjectiu d'aplicació del Sistema Intern d'informació

Pot accedir a presentar una comunicació a través del Canal del SIDI que s'implanta i regula per aquesta Instrucció, qualsevol persona informant de les legitimades a l'article 3 de la Llei 2/2023, en relació amb l'entitat XXXXXXXXXXX. A aquestes persones se'ls prestarà la protecció de l'informant que preveu la Llei 2/2023.

Article 6. Àmbit material del Sistema Intern d'informació

1. El SIDI de l'entitat XXXXX protegeix les persones físiques referides a l'article 3 de la Llei 2/2023 que, a través del Canal que s'habilita a l'efecte, informin de qualsevol de les accions o omissions detallades a l'article 2 de la Llei 2/2023, és dir:

    1) Accions o omissions que puguin constituir infraccions del dret de la Unió Europea sempre que:

        a. Entrin dins l'àmbit d'aplicació detallat a l'annex de la Directiva (UE) 2019/1937; o
        b. Afectin els interessos financers de la Unió Europea tal com es preveuen a l'article 325 del Tractat de Funcionament de la Unió Europea (TFUE); o
        c. Incideixin al mercat interior, tal com es preveu a l'article 26, apartat 2 del TFUE.

    2) Accions o omissions que puguin ser constitutives d'infracció penal o administrativa greu o molt greu. En tot cas, s'hi inclouen les que impliquin perjudici econòmic per a la Hisenda Pública i per a la Seguretat Social.

2. També es protegeix a les persones jurídiques en els termes previstos l'article 3.4.c) de la Llei 2/2023.

Article 7. Règim jurídic del Sistema Intern d'informació

L'organització i el funcionament del SIDI es regeix per la Llei 2/2023, de 20 de febrer, reguladora de la protecció de les persones que informin sobre infraccions normatives i de lluita contra la corrupció i per la Directiva (UE) 2019/1937 del Parlament Europeu i del Consell, del 23 d'octubre, per les normes aplicables de règim jurídic de les administracions públiques i procediment administratiu i normativa de protecció de dades personals i, en el marc normatiu assenyalat, per les determinacions contingudes en la present Instrucció.

Article 8. Drets i obligacions de la persona informant

1. Els drets mínims que, en el marc del SIDI, s'atribueixen a la persona informant són els següents:
    a) Disposar d'un Canal segur de comunicació que permeti presentar la informació per escrit o verbalment.
    b) Formular la comunicació de manera anònima o no anònima. En aquest segon cas, gaudirà del dret a la garantia de reserva de la identitat, que serà protegida i no podrà ser revelada. Aquest dret també s'estén als possibles testimonis

que intervinguin en la comprovació dels fets comunicats.

c) Protecció efectiva de la seva integritat laboral, sense que pugui patir represàlies ni ser discriminat o simplement assenyalat per raó de la informació comunicada.
d) Que es tramiti la seva informació i que s'obri una investigació exhaustiva, rigorosa, independent i autònoma.
e) Indicar una adreça electrònica, adreça postal o lloc segur a través del qual mantenir comunicació confidencial amb el Responsable del SIDI. Aquest dret pot ser renunciat expressament per la persona comunicant.
f) Ser informada sobre l'estat de la tramitació de informació comunicada (arxivament, derivació, elevació a òrgans superiors, etc.).
g) Gaudir i exercir els drets de protecció de dades personals previstos al Títol VI de la Llei 2/2023.
h) Gaudir de les mesures de protecció que previstes al Títol VII de la Llei 2/2023.

2. La persona informant té les obligacions que estableix la Llei 2/2023.

3. La presentació de la informació no atorga a la persona que la presenta, la condició d'interessat en l'expedient, tal com prescriu l'article 20.5 de la Llei 2/2023.

4. En cas que es facin públiques o es difonguin informacions falses, una vegada comprovades les circumstàncies, les terceres persones afectades o la mateixa entitat podran exercir les accions públiques i privades que estimin oportunes en defensa dels seus drets.

No obstant l'anterior, la protecció de l'informador prevista en aquesta Instrucció no es perd quan s'hagi comunicat informació inexacta per error comès de bona fe.

Article 9. Drets i obligacions de la persona afectada per la comunicació

1. Els drets mínims que, en el marc del SIDI, s'atribueixen a la persona afectada pels fets posats en coneixement de l'entitat:

a) Ser informada pel Responsable del SIDI de la comunicació que l'afecta, llevat que calgui mantenir el secret per a la millor comprovació dels fets.
b) Tractament confidencial de les seves dades personals i preservació de la seva identitat i dels fets i dades aportades. Aquest dret persisteix una vegada finalitzat el procediment incoat, tret que calgui comunicar les dades a petició de l'autoritat competent i prèvia posada en coneixement del denunciat.
c) Màxima reserva en les tasques de comprovació i respecte a la presumpció d'innocència.
d) Accés a l'expedient incoat arran de la comunicació de la persona informant, sense revelar informació que pogués identificar-la.
e) Presentar al·legacions en el format que millor consideri i ser escoltada en qualsevol moment.
f) Aportar els mitjans de prova que consideri pertinents
g) Dret de defensa i comparèixer a l'expedient assistit/da d'advocat.

2. La persona afectada per la comunicació té les obligacions que estableix la Llei 2/2023.

CAPÍTOL II. ÒRGANS I CANAL

Article 10. Responsable del Sistema Intern d'informació

1. En cas d'optar per òrgan col.legiat

   D'acord amb l'article 8.2 de la Llei 2/2023, es crea el Comitè Responsable del Sistema Intern d'Informació, òrgan col·legiat que assumirà les funcions i tindrà les garanties previstes a l'esmentada Llei pel "Responsable del Sistema d'Informació" (en endavant RSIDI). Aquest delegarà en un dels seus membres les facultats de gestió del SIDI i de tramitació d'expedients d'investigació. Les persones que el composaran seran els titulars de les unitats organitzatives i dels llocs de treball següents:

   - Persona delegada pel RSIDI per al suport a la gestió del Sistema Intern d'Informació i tramitació dels expedients d'investigació

   També assistirà, amb veu i sense vot, el Delegat de Protecció de Dades

   Les persones membres de l'òrgan col·legiat seran designades i, en el seu cas, destituïdes i cessades per la Presidència de la Diputació.

   1 BIS En cas d'optar per una persona física
   D'acord amb l'article 8.2 de la Llei 2/2023, es designa Responsable del Sistema Intern d'Informació, a la persona titular del lloc de treball de _____, que assumirà les funcions i tindrà les garanties previstes a l'esmentada Llei pel "Responsable del Sistema d'Informació" (en endavant RSIDI)

2. El RSIDI assumeix les funcions de direcció i es responsabilitza de les tasques de gestió del Sistema i de tramitació dels expedients d'investigació, d'acord amb el que es detalla a l'article següent.

3. En cas d'optar per òrgan col.legiat

   En l'exercici de les seves funcions el RSIDI i els seus membres actuaran amb independència i autonomia funcional sense que puguin estar sotmesos a ordres o instruccions que en condicionin l'actuació, especialment pel que fa al manteniment de la confidencialitat.

   BIS En cas d'optar per una persona física
   En l'exercici de les seves funcions el RSIDI actuarà amb independència i autonomia funcional sense que pugui estar sotmès a ordres o instruccions que en condicionin l'actuació, especialment pel que fa al manteniment de la confidencialitat.

El desenvolupament d'aquesta actuació no podrà ser causa que en justifiqui el cessament ni cap altra acció que es pugui interpretar com a repressiva.

4. El RSIDI i les persones que li donen suport estan subjectes al deure de confidencialitat i de protecció de dades personals en totes les fases del procediment. Aquest deure es manté un cop hagin cessat en les seves funcions.

5. El RSIDI i les persones que li donen suport han de ser funcionaris adscrits a l'entitat XXXXXXX o personal laboral fix de la mateixa, amb amplis coneixements de l'entitat, no poden tenir la condició de personal eventual i han de rebre formació específica per desenvolupar aquesta tasca.

Article 11. Funcions del Responsable del Sistema Intern d'Informació

1. El RSIDI té les funcions previstes a la Llei 2/2023 i les funcions operatives o procedimentals següents:

   a) Registrar i gestionar les denúncies rebudes pel Canal.
   b) Confirmar la recepció de les denúncies.
   c) Assumir la gestió operativa i la conservació del registre i base de dades creats a l'efecte.
   d) Assumir la responsabilitat de la instrucció, fer les comprovacions i recopilar, del denunciant o tercers, la informació per al contrast i versemblança dels fets denunciats.
   e) Garantir el dret de defensa i la confidencialitat de la persona o persones afectades pels fets denunciats.
   f) Decidir sobre l'admissió a tràmit de la comunicació o denúncia.
   g) Formular l'informe de recomanació que posa fi a la comprovació dels fets.
   h) Remetre amb caràcter immediat la informació a la persona titular de la Secretaria de l'entitat, a través de la Direcció de Serveis Jurídics (si existeix), per tal que aquesta en valori el seu trasllat, si és el cas, al Ministeri Fiscal si els fets poden ser indiciàriament constitutius de delicte o a la Fiscalia Europea si fos el cas o altre organisme que es consideri competent per tramitar-la.
   i) Elaborar una memòria anual respecte del funcionament del Sistema Intern d'informació.

2. Les funcions esmentades en l'anterior apartat, corresponen al RSIDI de l'entitat XXXXX i a tal efecte es podran adreçar a qualsevol persona de qualsevol d'aquesta entitat, que haurà de cooperar necessàriament amb el RSIDI en exercici de les seves funcions, per tal de requerir informació o d'altre tipus de col·laboració.

Article 12. Canal d'Accés al Sistema Intern d'informació

1. El Canal d'accés al SIDI permet fer comunicacions per escrit o verbalment (telefònicament o mitjançant sistema de missatgeria de veu) i permet rebre comunicacions anònimes.

2. A través d'aquest Canal l'entitat rebrà les comunicacions relatives a la mateixa.

3. Pel que fa les comunicacions escrites, quan aquestes siguin telemàtiques, l'accés al SIDI serà per mitjà de l'eina de Globaleaks que el Consorci Administració Oberta de Catalunya (Consorci AOC) posa a disposició dels ens locals. Cas que de l'establiment d'aquesta col·laboració es derivi la naturalesa d'encarregat o corresponsable del tractament de dades del Consorci AOC, caldrà formalitzar el corresponent acord de tractament Responsable de Tractament/Encarregat de Tractament o acord de corresponsabilitat del Tractament, segons procedeixi.

4. Sens perjudici del Canal d'accés telemàtic, serà possible presentar la comunicació verbalment via telefònica, per correu postal o presencialment en paper personant-se, la persona informant, a la Unitat de Registre-oficina d'assistència en matèria de registre corresponent *(o nom que pertoqui*). En l'acusament de rebuda a lliurar a la persona informant se l'informarà dels aspectes relacionats amb la Protecció de dades de caràcter personal que figuren al punt 5è d'aquest article.

   La persona informant també pot presentar la comunicació mitjançant sol·licitud de reunió presencial que es farà amb el RSIDI en el termini màxim de set dies, a comptar des que es tingui constància de la petició de l'interessat.

5. El Canal advertirà la persona informant que la seva comunicació, sigui per escrit o verbal, i les seves dades personals, seran tractades d'acord amb el que estableix el Reglament (UE) 2016/679 del Parlament Europeu i del Consell, de 27 d'abril de 2016 (RGPD), la Llei Orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digital (LOPDGDD) i les previsions específiques de la Llei 2/2023 en aquesta matèria.

CAPÍTOL III. PROCEDIMENT PER A LA GESTIÓ D'INFORMACIONS (Art. 9 Llei 2/2023)

Article 13. Recepció de la comunicació

1. Les comunicacions entraran al SIDI a través del Canal regulat a l'article 12.

2. Amb el consentiment previ de informant, les comunicacions verbals i les fetes en reunió presencial, es documentaran d'alguna de les maneres següents:

   a) Mitjançant un enregistrament de la conversa en un format segur, durador i accessible, o
   b) Mitjançant una transcripció completa i exacta de la conversa o reunió mantinguda, o de l'enregistrament temporal, realitzada pel personal responsable de tractar-la confidencialment. S'oferirà a la persona informant l'oportunitat de comprovar, rectificar i acceptar la transcripció de la conversa. En el cas de la transcripció de l'enregistrament temporal, un cop acceptada la transcripció realitzada es procedirà immediatament a la destrucció de l'enregistrament.

3. En fer la comunicació, la persona informant podrà indicar un domicili, correu electrònic o lloc segur per rebre les notificacions. En cas que no inclogui aquesta indicació podrà renunciar a la recepció d'informació de les actuacions que es duen a terme arran de la comunicació que ha presentat.

4. El RSIDI podrà mantenir la comunicació amb la persona informant i, si ho considera necessari, sol·licitar-li informació addicional

5. Quan la comunicació hagi estat remesa per canals diferents al Canal regulat a l'article 12 o a persones de la corporació no responsables del seu tractament, el receptor de la comunicació ha de remetre-la immediatament al RSIDI sense revelar a cap altra persona qualsevol informació que pogués permetre identificar a la persona informant o a les persones afectades, atesa la tipificació de infracció molt greu del trencament de la confidencialitat, en aplicació de l'article 63.1.c) de la Llei 2/2023.

Article 14. Registre d'entrada al Sistema Intern d'informació

1. Presentada la informació, es registrarà al SIDI de l'entitat i se li assignarà número d'entrada i codi d'expedient restringit.

2. El SIDI estarà dotat d'una base de dades segura i d'accés restringit exclusiu per al RSIDI i la unitat que li doni suport, on s'hi registraran totes les comunicacions rebudes amb les següents dades:

   a) Data de recepció.
   b) Entitat receptora de la comunicació
   c) Codi d'identificació.
   d) Actuacions desenvolupades.
   e) Informe de recomanació que posa fi a la comprovació.
   f) Altres mesures adoptades.
   g) Data de tancament.

3. La base de dades segura del SIDI contindrà, a més del registre de les informacions rebudes, la informació detallada en l'anterior apartat, amb detall de les investigacions internes a què hagin donat lloc, garantint, en tot cas, els requisits de confidencialitat previstos en la Llei 2/2023.

   D'acord amb l'anterior, aquest registre no serà públic i només s'hi donarà accés prèvia petició de l'Autoritat judicial o d'investigació competent.

4. Les dades personals relatives a les informacions rebudes i a les investigacions internes només s'han de conservar durant el període que sigui necessari d'acord amb els articles 26 i 32 de la Llei 2/2023.

Article 15. Expedient restringit

En cas que no es disposi d'altra sistema específic independent, els expedients incoats al SIDI de l'entitat per a la gestió, tramitació i resolució d'alertes referides a la mateixa

entitat, seran tractats mitjançant expedients d'accés restringit als que només tindran accés el RSIDI i les persones que li donin suport que el RSIDI habiliti expressament.

Article 16. Acusament de rebuda

En el termini de set dies naturals des que es rebi la comunicació, el RSIDI o unitat de suport, n'acusarà la rebuda a la persona informant, tret que aquesta expressament hagi renunciat a rebre comunicacions o que el RSIDI consideri raonablement que l'acusament de rebuda pugui posar en perill la confidencialitat de la comunicació.

En l'acusament de rebuda de la comunicació s'inclourà la informació relativa a la protecció de dades personals en els termes previstos a l'art. 12.5 d'aquesta Instrucció, i de les mesures de protecció personal que es posen a disposició de la persona informant en els termes previstos a la Llei 2/2023.

Article 17. Admissió

1. Una vegada registrada la comunicació, el RSIDI ha de comprovar si exposa fets o conductes que es troben dins l'àmbit de l'article 6 d'aquesta Instrucció.

2. Realitzada aquesta anàlisi preliminar, el RSIDI decidirà en un termini màxim de deu dies hàbils des de la data de registre de la comunicació, i prenent com a criteris els previstos a l'article 18.2 de la Llei 2/2023, si:

   a) Inadmet la comunicació:

      1r. Quan els fets exposats no tinguin prou versemblança o fonament.

      2n. Quan els fets exposats no siguin constitutius d'infracció de l'ordenament jurídic inclosa a l'àmbit d'aplicació de la Llei 2/2023.

      3r. Quan hagi indicis raonables d'haver-se obtingut la informació mitjançant la comissió d'algun delicte. En aquest cas a més de la inadmissió, el RSIDI n'informarà a la persona titular de la Secretaria de l'entitat, a través de la Direcció de Serveis Jurídics (si existeix), perquè pugui valorar la seva remissió, si és el cas, al Ministeri Fiscal.

      4t. Quan la comunicació no aporti informació nova o significativa en relació amb una comunicació anterior de la que ja hagi conclòs el procediment, tret que es donin noves circumstàncies que justifiquin un seguiment diferent.

      En cas d'inadmissió a tràmit, aquesta s'ha de comunicar a l'informant dins dels deu dies hàbils posteriors a la data de registre de la comunicació, tret que la comunicació sigui anònima o l'informant hagi renunciat a rebre comunicacions respecte de la tramitació.

   b) Admet a tràmit la comunicació, perquè no es troba en cap dels supòsits de l'apartat a anterior.

   c) Remet amb caràcter immediat la comunicació a la persona titular de la

Secretaria de l'entitat, a través de la Direcció de Serveis Jurídics (si existeix), perquè en valori el seu trasllat, si és el cas, al Ministeri Fiscal si els fets poden ser indiciàriament constitutius de delicte o a la Fiscalia Europea si fos el cas.

d) Remet la comunicació a la persona titular de la Secretaria de l'entitat, a través de la Direcció de Serveis Jurídics (si existeix), perquè en valori la seva remissió a l'entitat o l'organisme que consideri competent per tramitar-la.

Article 18. Instrucció

1. La instrucció comprèn totes les actuacions encaminades a comprovar la versemblança dels fets exposats en la comunicació registrada.

2. El RSIDI contactarà, de manera confidencial, amb la o les persones afectades per la informació, per assabentar-la que s'ha rebut la comunicació i remetre-li una breu exposició dels fets que es comuniquen. D'aquest tràmit se'n deixarà constància a la instrucció de l'expedient.

3. El RSIDI informarà a la persona afectada dels drets mínims que té, que són els relacionats a l'article 9.1 d'aquesta Instrucció.

   En cap cas el RSIDI no comunicarà ni donarà accés a la o les persones afectades, a informació que pugui identificar la persona informant.

4. S'integrarà a l'expedient d'instrucció l'aportació d'al·legacions i/o mitjans de prova per qualsevol de les persones informants o afectades i serviran per a la fonamentació de la proposta de resolució i la resolució de l'expedient.

5. Si és possible, en aquesta fase d'instrucció, el RSIDI mantindrà una entrevista amb la/es persona/es afectada/es, perquè pugui/n exposar la seva versió dels fets.

6. La instrucció serà dirigida i responsabilitat del RSIDI qui, en concloure-la, elaborarà proposta d'actuació per a la resolució dels fets comunicats.

Article 19. Protecció de la persona afectada

1. Una vegada confirmada la versemblança de la informació, la persona o persones afectades gaudiran de tracte confidencial i de protecció de les seves dades personals durant la tramitació de l'expedient, garantint que, en tot moment del tractament de l'alerta, la informació serà tractada de manera segura i aliena qualsevol intromissió.

2. Les persones afectades per la informació comunicada tindran dret a ser informades de les accions o omissions que li son atribuïdes i a ser escoltades en qualsevol moment. Aquest dret s'exercirà en el temps i la forma adequats per garantir el bon fi de la investigació.

3. D'acord amb l'article referent als drets de les persones afectades, es respectarà en tot cas la seva presumpció d'innocència i honor.

Article 20. Finalització i tractament

1. Concloses les actuacions d'instrucció, el RSIDI, prenent com a criteris els previstos a l'article 20.2 de la Llei 2/2023, emetrà un informe-proposta d'actuació per a la resolució dels fets comunicats que contindrà, almenys:

   a) Identificació de l'entitat, codi d'identificació de la comunicació, data de registre i exposició dels fets comunicats.

   b) Actuacions realitzades per comprovar la versemblança dels fets.

   c) Conclusions deduïdes en la instrucció, valoració de les diligències i dels indicis.

   d) Proposta d'actuació, que serà en un dels sentits següents:

      i. Arxiu de l'expedient, que serà notificat a la persona informant i, si escau, a la persona afectada. En aquests supòsits, l'informant tindrà dret a la protecció prevista per la Llei 2/2023, tret que es conclogui que la comunicació havia d'haver estat inadmesa.
      ii. Remetre la comunicació i les actuacions d'instrucció a la persona titular de la Secretaria de l'entitat, a través de la Direcció de Serveis Jurídics (si existeix), perquè en valori la seva remissió, si és el cas, al Ministeri Fiscal si els fets poden ser indiciàriament constitutius de delicte o a la Fiscalia Europea di fos el cas.
      iii. Remetre la comunicació i les actuacions d'instrucció a la persona titular de la Secretaria de l'entitat, a través de la Direcció de Serveis Jurídics (si existeix), perquè en valori la seva remissió a l'entitat o l'organisme que consideri competent per tramitar-la.
      iv. Adopció d'acord d'inici d'actuacions internes en forma de procediment disciplinari o sancionador en els termes legalment previstos, que serà instruït i resolt per l'òrgan que ordinàriament tingui atribuïda la competència.

2. El termini per finalitzar les actuacions d'instrucció i donar resposta a la persona informant, si és el cas i sempre que els fets no presentin indicis de delicte, no pot ser superior a tres mesos a comptar des de l'entrada al registre de la informació. Llevat de casos d'especial complexitat que requereixin una ampliació del termini, en aquest cas es podrà ampliar el termini fins a un màxim d'altres tres mesos addicionals per al correcte esclariment dels fets, sense perjudici de la remissió d'actuacions a entitats o organismes externs competents.

Article 21. Inici d'actuacions internes

1. Quan, com a conseqüència de la instrucció de l'expedient restringit realitzada pel RSIDI, s'hagi adoptat un acord per a l'inici d'actuacions internes, el RSIDI podrà donar accés de l'expedient restringit on consta la instrucció i investigació, a les persones de l'ens del sector públic, segons el cas, següents:

   a) La persona que ocupi la direcció de recursos humans o persona d'aquest àmbit

designada degudament, quan pugui procedir l'adopció de mesures disciplinàries contra un treballador.

b) La persona que ocupi la direcció dels serveis jurídics o persona d'aquest àmbit designada degudament, quan pugui procedir l'adopció de mesures legals en relació amb els fets relatats a la denúncia o alerta.

c) Les persones encarregades del tractament de l'assumpte que eventualment es designin.

d) El delegat de protecció de dades.

2. En l'expedient on es materialitzin les actuacions internes, en tot cas, es garantirà la confidencialitat de la persona informadora, la identitat de la qual només podrà ser facilitada quan ho requereixi motivadament l'Autoritat externa competent a qui s'hagués de donar trasllat.

   Tret que l'Autoritat externa ho impedeixi, abans de facilitar les dades identificatives de la persona informant, aquesta serà informada dels fets amb la motivació explícita que ho justifiqui.

CAPÍTOL IV. TRANSPARÈNCIA, PUBLICITAT I PROTECCIÓ

Article 22. Difusió del sistema Intern d'informació

1. La present Instrucció d'implantació del SIDI es publicarà a la pàgina web de l'entitat, on hi haurà informació clara i accessible del seu funcionament, de la protecció que es dona a la persona informant i de l'enllaç al Canal d'entrada al SIDI, com també de la resta d'extrems previstos a l'article 25 de la Llei 2/2023 segons resulti d'aplicació.

   S'hi inclourà també l'enllaç al canal extern de denúncies de l'Oficina Antifrau de Catalunya i, en aquest mateix espai, es publicitarà el nombre total anual d'informacions rebudes a través del SIDI.

2. L'entitat farà difusió del seu SIDI per tal que en pugui tenir coneixement tot el personal que hi presta servei així com tots aquells tercers que estan o han estat vinculats o relacionats amb la ella.

Article 23. Protecció de dades personals

a) Règim jurídic del tractament de dades personals.

Els tractaments de dades personals que derivin de l'aplicació de la Llei 2/2023 es regeixen per allò que es disposa al Reglament (UE) 2016/679 del Parlament Europeu i del Consell, de 27 d'abril de 2016 (RGPD), a la Llei Orgànica 3/2018, de 5 de desembre, de Protecció de Dades Personals i garantia dels drets digitals (LOPDGDD), a la Llei Orgànica 7/2021, de 26 de maig, de protecció de dades personals tractades per a finalitats de prevenció, detecció, investigació i enjudiciament d'infraccions penals i de execució de sancions penals (Llei Orgànica 7/2021) i en el Títol VI de la Llei 2/2023.

No es recopilaran dades personals la pertinència de les quals no resulti manifesta per a tractar una informació específica o, si es recopilen per accident, s'eliminaran sense dilació indeguda.

b) Licitud dels tractaments de dades personals.

1. Es consideren lícits els tractaments de dades personals necessàries per aplicar la Llei 2/2023.
2. El tractament de dades personals, en els supòsits de comunicació interns, s'entendrà lícit en ser obligatori disposar d'un SIDI.
3. El tractament de les categories especials de dades personals per raons d'un interès públic essencial es pot fer d'acord amb el que preveu l'article 9.2.g) de l'RGPD.

c) Informació sobre protecció de dades personals i exercici de drets.

1. Quan s'obtinguin directament de les persones interessades les seves dades personals se'ls facilitarà la informació a què es refereixen els articles 13 de l'RGPD i 11 de la LOPDGDD.

   A les persones informants se'ls informarà, a més, de manera expressa, que la seva identitat serà en tot cas reservada, que no es comunicarà a les persones a què es refereixen els fets relatats ni a tercers.

2. La persona a què es refereixin els fets relatats no serà en cap cas informada de la identitat de la persona informant.

3. Els interessats poden exercir els drets a què fan referència els articles 15 a 22 de l'RGPD.

4. En cas que alguna de les persones què es refereixin els fets relatats en la comunicació exerceixi el dret d'oposició, es presumeix que, llevat de prova en contra, hi ha motius legítims imperiosos que legitimen el tractament seves dades personals.

d) Tractament de dades personals al SIDI.

1. L'accés a les dades personals contingudes al Sistema intern d'informació de l'entitat queda limitat, dins l'àmbit de les seves competències i funcions, exclusivament a:

   a) El RSIDI i qui el gestioni directament.
   b) La persona responsable de recursos humans o l'òrgan competent designat degudament, només quan pugui procedir l'adopció de mesures disciplinàries contra un treballador. En el cas dels empleats públics, l'òrgan competent per a la tramitació del mateix.
   c) La persona responsable dels serveis jurídics de l'entitat (si existeix), si escau l'adopció de mesures legals en relació amb els fets relatats a la comunicació.
   d) Els encarregats del tractament que eventualment es designin.
   e) El delegat de protecció de dades de l'entitat.

2. És lícit el tractament de les dades per altres persones, o fins i tot la seva comunicació a tercers, quan sigui necessari per a l'adopció de mesures correctores a l'entitat o la tramitació dels procediments sancionadors o penals que, si escau, siguin procedents.

   En cap cas seran objecte de tractament les dades personals que no siguin necessàries per al coneixement i la investigació de les accions o omissions a què es refereix l'article 2 de la Llei 2/2023, i es procedirà, si s'escau, a la seva supressió immediata. Així mateix, se suprimiran totes aquelles dades personals que es puguin haver comunicat i que es refereixin a conductes que no estiguin incloses a l'àmbit d'aplicació de la llei.

   Si la informació rebuda conté dades personals incloses dins de les categories especials de dades, se'n procedirà a la supressió immediata, sense que es procedeixi al registre i tractament d'aquestes.

3. Les dades que siguin objecte de tractament es poden conservar al sistema d'informacions únicament durant el temps imprescindible per decidir sobre la procedència d'iniciar una investigació sobre els fets informats.

   Si s'acredités que la informació facilitada o part d'aquesta no és veraç, s'ha de procedir a suprimir-la immediatament des del moment en què es tingui constància d'aquesta circumstància, llevat que aquesta manca de veracitat pugui constituir un il·lícit penal, cas en què es guardarà la informació pel temps necessari durant el qual es tramiti el procediment judicial.

4. En tot cas, transcorreguts tres mesos des de la recepció de la comunicació sense que s'hagin iniciat actuacions de recerca, s'haurà de procedir a la seva supressió, llevat que la finalitat de la conservació sigui deixar evidència del funcionament del sistema. Les comunicacions a què no s'hagi donat curs només podran constar de forma anonimitzada, sense que sigui aplicable l'obligació de bloqueig prevista a l'article 32 de la Llei orgànica 3/2018, de 5 de desembre.

5. Els empleats i tercers han de ser informats sobre el tractament de dades personals

en el marc del SIDI a que fa referència aquesta Instrucció .

e) Preservació de la identitat de l'informant i de les persones afectades.

1. Qui presenti una comunicació té dret que la seva identitat no sigui revelada a terceres persones.

2. Els sistemes interns d'informació no obtindran dades que permetin la identificació de l'informant i han de tenir mesures tècniques i organitzatives adequades per preservar la identitat i garantir la confidencialitat de les dades corresponents a les persones afectades i a qualsevol tercer que s'esmenti a la informació subministrada, especialment la identitat de l'informant en cas que s'hagués identificat.

3. La identitat de l'informant només es pot comunicar a l'Autoritat judicial, al Ministeri Fiscal o a l'autoritat administrativa competent en el marc d'una investigació penal, disciplinària o sancionadora.

Les revelacions fetes en virtut d'aquest apartat estaran subjectes a salvaguardes establertes a la normativa aplicable. En particular, s'ha de traslladar a l'informant abans de revelar-ne la identitat, llevat que aquesta informació pogués comprometre la investigació o el procediment judicial. Quan l'autoritat competent ho comuniqui a l'informant, li remetrà un escrit explicant els motius de la revelació de les dades confidencials en qüestió.

f) Registre d'Activitats de Tractament

Atesa la seva singularitat en relació amb la resta d'Activitats de Tractament, el tractament relatiu a la *gestió del Sistema Intern d'informació de l'entitat XXXXXX, previst 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,* s'incorporarà com a Activitat de Tractament específica al Registre d'Activitats de Tractament de l'entitat, quina descripció i continguts mínims seran els establerts a l'article 30 RGPD.

Article 24. Mesures de protecció i suport a les persones

S'aplicaran les mesures de protecció i suport previstes al Títol VII de la Llei 2/2023.

7.2 Anexo 02

RESOLUCIÓ 49/2023

ACORD D'APROVACIO DE L'ADAPTACIÓ DEL CANAL DE CONDUCTA DE LA XARXA AUDIOVISUAL LOCAL, SL A LA NOVA LLEI 2/2023 DE PROTECCIÓ DE LES PERSONES QUE INFORMIN SOBRE INFRACCIONS NORMATIVES I DE LLUITA CONTRA LA CORRUPCIÓ

Antecedents

12. La Directiva (UE) 2019/1937 del Parlament Europeu i del Consell de 23 d'octubre (en endavant Directiva 2019/1937), amb la finalitat de reforçar l'aplicació del Dret i les polítiques de la Unió Europea mitjançant l'establiment d'unes normes mínimes comunes que proporcionin un nivell de protecció a les persones que informin sobre infraccions del Dret de la Unió, obliga a les entitats jurídiques del sector públic i privat a establir canals i procediments de denúncia interna i de seguiment.

13. La Llei 2/2023, de 20 de febrer, reguladora de la protecció de les persones que informin sobre infraccions normatives i de lluita contra la corrupció (en endavant Llei 2/2023) transposa la Directiva (UE) 2019/1937 a l'ordenament espanyol. La Llei obliga als ens dels sector públic i del sector privat a la implantació d'un Sistema intern d'informació que permeti a les persones que en un context laboral o professional detectin infraccions penals o administratives greus o molt greus, posar-les en coneixement mitjançant els mecanismes que s'hi regula. La finalitat de la norma és la de protegir a aquestes persones que informin, específicament, sobre infraccions del Dret de la Unió previstes a l'esmentada Directiva (UE) 2019/1937 i infraccions penals i administratives greus i molt greus de l'ordenament jurídic intern.

14. Aquesta regulació del dret estatal compta amb antecedents, com ho són l'article 24.1 de la Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals, en referència a les entitats de dret privat. Així com el Reial decret llei 11/2018, del 31 d'agost, que va introduir a la Llei 10/2010, del 28 d'abril, de prevenció del blanqueig de capitals i del finançament del terrorisme. En coherència amb aquest context, la Llei 2/2023 preveu la presentació de denúncies anònimes i obliga, en tot cas i de conformitat amb la Directiva (UE) 2019/1937, a la protecció de l'informant i a la preservació de la seva confidencialitat.

15. En quant a l'obligatorietat de disposar del Sistema intern d'informació que prescriu la Llei 2/2023, el seu article 13 disposa que totes les entitats que integren el sector públic, sense excepció, estan obligades a disposar de Sistema intern d'informació. És el cas de les entitats pertanyents al sector públic amb personalitat jurídica pròpia vinculades o dependents que tinguin 50 treballadors o més.

16. La Xarxa Audiovisual Local, SL (XAL) és una societat mercantil limitada de capital íntegrament públic de la Diputació de Barcelona creada per a la gestió del servei públic de caràcter econòmic de suport i foment de la comunicació audiovisual local. La

XAL amb aquest objectiu, gestiona La Xarxa de Comunicació Local, una plataforma única de continguts multimèdia i serveis adreçats als mitjans de comunicació locals.

17. La Xarxa Audiovisual Local, SL (XAL) ja compta amb un canal de denúncia i un comité de conducta per a la gestió de les posibles denúncies creat per Acord del Consell d'administració de 20 de desembre de 2018.

18. La Xarxa Audiovisual Local, SL (XAL) com a ens del sector públic dependent i vinculat a la Diputació de Barcelona de 50 treballadors o més, de conformitat amb la mateixa Llei 2/2023, han d'adoptar els seu propi Sistema intern d'informació, dotar-lo de recursos per a les investigacions i tramitacions i designar el seu responsable. Per a fer-ho la XAL aprofitarà els òrgans existents adaptant-los a la normativa vigent.

19. Per acord núm. 33 del ple de 24 de febrer de 2022, la Diputació de Barcelona va aprovar el Sistema d'Integritat Institucional i Pla de mesures antifrau de la Diputació i dels ens del seu sector públic que s'hi puguin adherir, el qual va ser actualitzat per acord núm. 42 de la sessió plenària de 23 de febrer de 2023. La XAL ha sol·licitat l'adhesió a aquest sistema.

20. D'acord amb el context corporatiu i comptant actualment amb un marc legal estatal que prescriu l'obligatorietat d'establir el Sistema intern d'informació, la XAL ha impulsat diverses accions per dotar-se dels requeriments mínims legalment previstos i per a la posada en funcionament del Sistema dins del termini establert en l'esmentada disposició transitòria segona de la Llei 2/2023, això és, en el termini de tres mesos a comptar des de l'entrada en vigor de la Llei el passat 13 de març, termini que s'exhaureix el proper 13 de juny.

21. Entre les anteriors accions, en primer terme, s'han elaborat els documents "Política del sistema intern d'informació" i "Procediment de gestió del sistema intern d'informació" que ha estat sotmesa al tràmit de prèvia consulta amb la representació legal de les persones treballadores en data 9 de juny.

22. En segon terme, s'ha treballat en determinar quina ha de ser l'eina tecnològica que permeti la presentació d'informacions al Sistema, és dir el canal intern d'informació, previst als articles 5 i 7 de la Llei 2/2023. Aquests treballs s'han emmarcat en la col·laboració que la Diputació té establerta amb la Xarxa de Governs Oberts (XGO) i, en el si d'aquesta, amb el Consorci Administració Oberta de Catalunya (Consorci AOC), a qui s'ha sol·licitat l'alta en el Servei de "Bústia ètica" que permet l'establiment del canal per informar d'infraccions normatives complint amb els requisits legals i emprant el programari de codi obert Globaleaks, integrat en el catàleg de serveis del Consorci AOC.

    Així mateix, aquest Servei "Bústia ètica" permet l'elaboració del formulari per a la presentació de les comunicacions o alertes que poden ser també anònimes, de conformitat amb el previst a la Llei 2/2023.

23. Així mateix, i en compliment del disposat a l'article 25 de la Llei 2/2023, es preveu proporcionar informació de manera clara i accessible sobre l'ús del canal intern a la

pàgina web de l'entitat, així com dels principis essencials que preveu el document "Política del sistema intern d'informació".

Fonaments de dret

La normativa específica en la que es fonamenta jurídicament aquesta resolució està constituïda per:

5. La Directiva (UE) 2019/1937 del Parlament Europeu i del Consell, de 23 d'octubre, relativa a la protecció de les persones que informin sobre infraccions del Dret de la Unió, estableix l'obligació als Estats membres de transposar la norma al Dret nacional.

6. La Llei 2/2023, de 20 de febrer, reguladora de la protecció de les persones que informin sobre infraccions normatives i de lluita contra la corrupció, que transposa a l'ordenament jurídic espanyol la Directiva (UE) 2019/1937 del Parlament Europeu i del Consell.

7. En concordança amb l'establert al títol VI de l'esmentada Llei 2/2023, és d'aplicació la Llei orgànica 3/2018, de 5 de desembre, de protecció de dades personals i garantia dels drets digitals que, entre d'altres, transposa al dret estatal el Reglament (UE) 2016/679 del Parlament Europeu i del Consell, de 27 d'abril de 2016, relatiu a la protecció de les persones físiques pel que fa al tractament de les dades personals.

8. En compliment de la DA 7a de la Llei 3/2023, de 16 de març, de mesures fiscals, financeres, administratives i del sector públic per al 2023, s'ha de donar trasllat a l'Oficina Antifrau de Catalunya de la present resolució, atesa la seva condició d'Autoritat Administrativa Independent (AAI).

L'adopció d'aquesta resolució es justifica en la circumstància d'haver de donar compliment al termini previst a la disposició transitòria segona de la Llei 2/2023 que s'exhaureix el proper 13 de juny de 2023, raó per la qual la seva tramitació no es pot ajornar sense que se'n derivi un perjudici rellevant per a l'interès públic que impulsa l'actuació de la XAL.

Atès que l'article 14è dels Estatuts de la societat disposen que la societat estarà regida, administrada i representada pel Consell d'Administració, el qual exercirà totes aquelles facultats no reservades expressament a la Junta General i a la Gerència per la Llei o els Estatuts, i en especial ostentarà l'administració i representació, tant judicial com extrajudicial, amb les més àmplies facultats de gestió, administració i disposició, per a tota classe d'actes i contractes compresos a l'objecte social i que l'article 14.6 determina que el Consell podrà designar d'entre els seus membres un Conseller delegat.

Vist que el Consell d'administració de la societat en la sessió celebrada el 31 de març de 2022 va nomenar el Sr. Marc Melillas Esquirol, Conseller delegat de Xarxa Audiovisual Local, SL, acord que va ser protocolitzat a l'escriptura de nomenament, autoritzada pel Notari de Barcelona, Sr. Lluís Jou i Miravent, en data 7 d'abril de 2022, amb número de protocol 699.

En virtut de tot això, i de conformitat amb el que estableixen els Estatuts de la Xarxa Audiovisual Local, SL, el Conseller Delegat de la XAL, SL,

RESOL

Primer. Aprovar la "Política del Sistema Intern d'Informació" i el "Procediment de gestió del Sistema Intern d'Informació" que s'adjunten com a **Annex 1 i 2**.

Segon. Nomenar com a responsable del Sistema Intern d'Informació el Comitè de conducta
de la XAL nomenat pel Consell d'administració de la XAL del 20 de desembre de 2018.

Tercer. DISPOSAR que la presentació de les informacions a què es refereix aquesta resolució s'haurà de vehicular a través de l'eina subministrada pel Consorci AOC disponible en el seu catàleg de serveis, tot i mantenir el canal de denuncia previst en el Codi de Conducta de l'entitat.

Quart. FER DIFUSIÓ de la "Política del Sistema Intern d'Informació" i el "Procediment de gestió del Sistema Intern d'Informació que s'aproven amb la present resolució.

Cinquè. ESTABLIR l'obligatorietat d'observança de la Instrucció per a la implantació i gestió del Sistema intern d'informació per part de tots el personal i directius de la XAL.

Sisè. DONAR TRASLLAT a l'Oficina Antifrau de Catalunya (AAI) de la present resolució.

Setè. DONAR COMPTE al Consell d'administració de la XAL.

Annex 1

POLÍTICA DEL SISTEMA INTERN D'INFORMACIÓ

la xarxa
comunicació local

Contingut

Introducció

La Llei 2/2023, de 20 de febrer, reguladora de la protecció de les persones que informin sobre infraccions normatives i de lluita contra la corrupció, estableix la necessitat de disposar d'un Sistema Intern d'Informació, com a via preferent per informar sobre les accions o omissions que puguin constituir infraccions penals o administratives greus o molt greus.

Alhora, l'existència d'un Sistema Intern d'Informació constitueix una expressió del compromís de la XARXA AUDIOVISUAL LOCAL, S.L. (en endavant "La XAL") amb la integritat i el comportament ètic en tots els seus àmbits d' actuació.

Per això, el Conseller delegat ha aprovat la present **Política del Sistema Intern d'Informació** en la qual s'identifiquen els canals de denúncia i els drets i garanties que assisteixen als informants i a totes les persones afectades per una denúncia.

El Conseller delegat ha designat un **Responsable del Sistema Intern d'Informació**, dotat d'independència i poders autònoms de supervisió i control per garantir el correcte funcionament del Sistema Intern d'Informació.

1. Àmbit d' aplicació

1.1. **Àmbit d'aplicació material:** El Sistema Intern d'Informació podrà utilitzar-se per denunciar o comunicar les següents conductes:

- Les accions o omissions que puguin ser constitutives d'infracció penal o infracció administrativa greu o molt greu.
- Qualsevol acció o omissió que pugui constituir infracció del Dret de la Unió Europea.

En el cas dels empleats de La XAL, hauran també de denunciar o comunicar qualsevol indici raonable de la comissió d'alguna irregularitat o d'algun acte contrari al Codi de Compliance o a la normativa interna.

1.2. **Àmbit d'aplicació personal:** Podran realitzar denúncies o comunicacions preferentment a través del Sistema Intern d'Informació, totes aquelles persones que hagin obtingut informació sobre infraccions en el context laboral o professional de la companyia:

- Els empleats de la companyia amb independència del seu nivell jeràrquic, de la naturalesa de la seva relació contractual i de la seva ubicació geogràfica o funcional.
- Els autònoms.
- Els membres de l'òrgan d'administració, direcció o supervisió de la companyia.
- Qualsevol persona que treballi per o sota la supervisió i direcció de contractistes, subcontractistes i proveïdors de la companyia.

També podran presentar denúncies o comunicacions les persones que hagin mantingut una relació laboral o estatutària ja finalitzada, voluntaris, becaris, treballadors en períodes de formació amb independència que percebessin o no una remuneració, així com a aquelles persones la relació laboral de les quals encara no hagi començat, en els casos en què la informació sobre infraccions hagi estat obtinguda durant el procés de selecció o de negociació precontractual.

2. Principis del Sistema Intern d'Informació:

2.1. **Garantia d'accés**: El Sistema Intern d'Informació garanteix a totes les persones referides a l'apartat anterior, la possibilitat de comunicar informació sobre les possibles infraccions descrites a l'apartat 1.1 de la present Política, de les quals tinguin informació o constància.

2.2. **Confidencialitat:** El Sistema Intern d'Informació es gestiona de forma segura, de manera que es garanteix la confidencialitat de la identitat de l'informant i de

qualsevol tercer esmentat en la comunicació o denúncia i de la tramitació d'aquesta.

La identitat de la persona que realitza la comunicació tindrà la consideració d'informació confidencial i, per tant, no serà revelada, sense el seu consentiment, a la persona o persones afectades, impedint l'accés de personal no autoritzat.

No obstant això, les dades de les persones que realitzen la comunicació podran ser facilitades a autoritats administratives o judicials competents, en la mesura que fossin requerides com a conseqüència de qualsevol procediment derivat de l'objecte de la comunicació. La cessió de dades a les autoritats administratives o judicials es realitzarà sempre donant ple compliment a la legislació sobre protecció de dades de caràcter personal.

2.3. **Protecció de dades personals:** Es garanteix la protecció de dades personals, impedint l'accés a la informació continguda en el Sistema Intern d'Informació per persones no autoritzades.

2.4. **Protecció de l'informant i garantia de no represàlia:** El Sistema Intern d'Informació garanteix la protecció de l'informant enfront de possibles represàlies directes o indirectes relacionades amb la presentació d'una comunicació en l'àmbit del Sistema.

2.5. **Drets de la persona afectada:** Durant la tramitació i especialment en el procés d'investigació i comprovació dels fets comunicats, es garantiran els drets a la intimitat, a la defensa i a la presumpció d'innocència de les persones afectades. La persona afectada per la denúncia o comunicació tindrà dret que se li informi de les accions o omissions que se li atribueixen i a ser escoltada en qualsevol moment. La comunicació tindrà lloc en el temps i forma que es consideri adient per garantir el bon fi de la recerca.

2.6. **Bona fe:** Les comunicacions i denúncies hauran de ser efectuades de bona fe. Es prohibeix la presentació de comunicacions i denúncies vinculades a conflictes

interpersonals o que es basin en intenció de difamació o perjudici a una altra persona.

3. Mitjans per a la presentació d'una denúncia o comunicació

3.1. Las persones descrites en el punt 1.1. de la present Política enviarà una comunicació mitjançant la plataforma habilitada a l'efecte, en la que s'haurà de fer constar la **següent informació** mínima:

a) Informació relativa a l'informant:
   - Identificació personal.
   - Correu electrònic.
   - En cas que realitzi la comunicació en nom d'una persona jurídica, dades de l'empresa (denominació, domicili, NIF i telèfon).

b) Informació relativa a la conducta comunicada:
   - Descripció dels fets.
   - Empleats o departaments afectats.

A sol·licitud de l'informant, podrà realitzar-se la denúncia o comunicació en una reunió presencial en el termini màxim de set (7) dies des de la seva sol·licitud o requeriment.

3.2. **Comunicacions anònimes**: No obstant això, el que disposa l'apartat anterior, es permeten les comunicacions anònimes, si l'informant opta per l'anonimat. La comunicació serà acceptada, tot i que la tramitació d'aquesta pot quedar limitada davant la dificultat de contrastar la veracitat de la mateixa.

3.3. En la realització de comunicacions, els informants atendran sempre **criteris de veracitat i proporcionalitat.**

4. Canals externs d' informació.

El Sistema Intern d'Informació es constitueix com la via preferent per informar sobre les accions o omissions previstes a l'apartat 1 d'aquesta Política. No obstant això, en cas de risc de represàlia, s'informa sobre l'existència d'altres canals externs d'informació davant d'autoritats competents tant d'Espanya com de la Unió Europea, on les persones interessades podran fer arribar la seva comunicació si així ho desitgen:

- Unió Europea: OLAF, Oficina Anti-Frau: https://anti-fraud.ec.europa.eu/index_es

- Autoritat Independent de Protecció de l'Informant, AAI (pendent de creació del canal).

- Oficina Antifrau de Catalunya: https://www.antifrau.cat/es/es

- Servei Nacional de Coordinació Antifrau: consultasantifraude@igae.hacienda.gob.es

5. Gestió del Sistema Intern d' Informació.

5.1. La companyia té encomanada la gestió del Sistema Intern d'Informació a un Expert Extern, qui assignarà a cada comunicació rebuda la corresponent codificació, acusarà rebut de la seva recepció i donarà el curs corresponent a la mateixa.

5.2. La tramitació de la denúncia o comunicació rebuda es realitzarà conforme al Procediment de gestió intern establert a l'efecte i respectant en tot cas els drets i garanties de totes les parts afectades.

6. Publicitat de la Política del Sistema Intern d' Informació.

La present Política es publicarà de la manera més oportuna a la pàgina web corporativa, així com a la intranet accessible als empleats.

7. Incompliment.

L'incompliment de la present Política, així com la realització deliberada de comunicacions o denúncies falses podrà implicar l'inici d'accions legals i/o disciplinàries, així com l'exercici d'accions que procedeixin en dret en defensa dels interessos de les persones afectades.

******

Annex 2

PROCEDIMENT DE GESTIÓ DEL SISTEMA INTERN D'INFORMACIÓ

Contingut

Introducció

El Conseller delegat de XARXA AUDIOVISUAL LOCAL, S.L. (en endavant LA XAL) ha aprovat una **Política del Sistema Intern d'Informació** en la qual es

recullen els drets i garanties que assisteixen als informants i a totes les persones afectades per una comunicació o denúncia.

Així mateix, el Conseller delegat ha aprovat el present **Procediment de gestió del Sistema Intern d'Informació** en el qual es recullen les normes de gestió de les comunicacions i denúncies rebudes.

1. Objecte i àmbit d'aplicació

El Procediment té per objecte establir les normes per a la gestió de les comunicacions i denúncies rebudes pels canals de denúncia de la companyia en l'àmbit del Sistema Intern d'Informació.
Aquest procediment aplica a totes les comunicacions i denúncies rebudes en el Sistema Intern d'Informació de la companyia, a través dels canals establerts, garantint la protecció deguda a l'informant i a les persones afectades per una comunicació o denúncia.

2. Procediment de gestió de denúncies i comunicacions

El Conseller delegat de La XAL ha designat un Responsable de la gestió del Sistema Intern d'Informació que vetlla pel bon funcionament del Sistema, la gestió de les comunicacions i denúncies rebudes.

La companyia té encomanada la gestió del Sistema Intern d'Informació a un Expert Extern.

Rebuda la comunicació o denúncia pels canals establerts a l'efecte, es remetrà a l'informant justificant de recepció en un termini no superior a set (7) dies naturals següents a la seva recepció, llevat que això pugui posar en perill la confidencialitat de la comunicació.

L'Expert Extern informarà al Responsable del Sistema Intern d'Informació que dirigirà la investigació interna que correspongui.

El Responsable designarà la persona o persones que duran a terme la investigació i que estaran subjectes a les obligacions de confidencialitat i imparcialitat.

La persona o les persones designades per tramitar l'expedient d'investigació adequaran aquesta a la legislació específica i normativa interna, que sigui d'aplicació al cas.

Amb caràcter previ a la seva tramitació, el Responsable del Sistema Intern d'Informació podrà requerir a l'informant en una o en diverses ocasions perquè faciliti informació addicional en relació amb els fets objecte de la comunicació o denúncia.

El termini màxim per donar resposta a les actuacions d'investigació no podrà ser superior a tres (3) mesos a comptar des de la recepció de la comunicació, excepte en casos d'especial complexitat que requereixin una ampliació del termini, en aquest cas el termini podrà estendre's fins a un màxim d'altres tres (3) mesos addicionals, sense perjudici dels terminis establerts en la legislació que sigui d'aplicació al cas.

3. Drets i garanties

Es garanteix la confidencialitat de la identitat de l'informant i de qualsevol tercer esmentat en la comunicació o denúncia, així com la confidencialitat en la seva tramitació.

En el cas de rebre's una comunicació o denúncia per canals diferents als establerts en la Política del Sistema Intern d'Informació o per persones diferents al Responsable del Sistema Intern d'Informació, aquestes han de guardar estricta confidencialitat i remetre immediatament la comunicació o denúncia al Responsable.

Es garanteix la protecció de dades personals, impedint l'accés a la informació per persones no autoritzades.

Les comunicacions i denúncies hauran de ser efectuades de bona fe. Es prohibeix la presentació de comunicacions i denúncies vinculades a conflictes interpersonals o que es basin en intenció de difamació o perjudici a una altra persona.

Quan el fet comunicat afecti el Responsable del Sistema Intern d'Informació, aquest no participarà en la seva tramitació i l'haurà d'advertir immediatament al Consell d'Administració de la companyia.

Durant la tramitació i especialment en el procés d'investigació i comprovació dels fets comunicats, es garantiran els drets a la intimitat, a la defensa i a la presumpció d' innocència de les persones afectades. La persona afectada per la denúncia o comunicació tindrà dret que se li informi de les accions o omissions que se li atribueixen i a ser escoltada en qualsevol moment. La comunicació tindrà lloc en el temps i forma que es consideri adient per garantir el bon fi de la recerca.

Es remetrà informació al Ministeri Fiscal amb caràcter immediat quan els fets poguessin ser indiciàriament constitutius de delicte.

4. Conservació de la documentació

Es portarà pel Responsable del Sistema Intern d'Informació un llibre registre en el qual constaran:

- Denúncies o comunicacions rebudes, amb la seva data i dades més rellevants.
- Informe de tramitació.
- Comunicacions amb l'informant i altres.
- Responsable de la tramitació.
- Informe final.
- Actuacions previstes o acordades.

En el llibre-registre es procurarà codificar els noms dels interessats per garantir la confidencialitat en totes les seves fases.

5. Seguiment del Sistema Intern d'Informació

El Responsable del Sistema Intern d'Informació elaborarà anualment un informe de funcionament on es recullin les dades sobre l'ús del Sistema, nombre de denúncies, resultats de les investigacions i altres informacions rellevants, així com possibles incidències en el seu funcionament. L'informe s'elevarà al Consell d'Administració.

****