

Respuesta a la consulta pública previa sobre la transposición de la DIRECTIVA (UE) 2019/1937 del Parlamento Europeo y del Consejo, de 23 de octubre de 2019, relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión (“WHISTLEBLOWERS” / ALERTADORES).

Realizada por Simona Levi en nombre de Xnet
Datos de contacto - email: xnet@xnet-x.net

Xnet (<https://xnet-x.net/eje/anticorrupcion/>) ha sido la primera organización, tanto en la Unión Europea como en España, en proponer un texto de transposición de la DIRECTIVA (UE) 2019/1937.

El texto, revisado por la organización de referencia Whistleblowing International Network (WIN) de la que Xnet es miembro (<https://whistleblowingnetwork.org/Home>), que integra las experiencias más rigurosas de otros países y adapta los elementos de la directiva europea profundizando en los aspectos que dependen de su transposición nacional, ha sido registrado como Proposición de Ley con el apoyo de más de 15 diputadas y diputados tanto en la XIII como en la presente legislatura en el Congreso de los Diputados (https://www.congreso.es/web/guest/proposiciones-de-ley?p_p_id=iniciativas&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view&iniciativas_mode=mostrarDetalle&iniciativas_legislatura=XIV&iniciativas_id=123/000003), donde, el 11 de diciembre de 2019, ha sido la primera Ley registrada al respecto. Su texto actualizado puede encontrarse en el siguiente enlace: <https://xnet-x.net/proposicion-ley-proteccion-integral-alertadores/>

En nuestro texto de Ley ya están contestadas todas estas preguntas. Para cada párrafo iremos contestando, indicando las partes de nuestra Proposición de Ley que hacen referencia a cada cuestión.

1. En relación con la facultad reconocida a los Estados miembros para ampliar la protección en su Derecho nacional a otros ámbitos o actos no previstos en el artículo 1.1 de la Directiva:

- ¿Debe ampliarse la protección del denunciante a cualquier materia del Derecho nacional más allá de la normativa con origen en el Derecho europeo?

[Premisa: **existe un error en la formulación de la pregunta** ya que esta facultad, en la Directiva se otorga en el artículo 2.2 y no el 1.1]

Sin dudas. Para garantizar una protección efectiva de las y los alertadores (denominados única y erróneamente a nuestro modo de ver como "denunciantes" en el documento relativo a la presente consulta pública), además de sus colaboradores, **es preciso utilizar la facultad otorgada a los Estados en el artículo 2.2 de la Directiva para ampliar el ámbito de aplicación material de la Directiva** ya que limitarlo simplemente a ilícitos relacionados con las normativa europea dejaría fuera la gran mayoría de casos de alertadores que ocurren en nuestro país y de este modo desactivaría de facto el espíritu de la normativa que, para mejorar la rendición de cuentas, la transparencia y la gobernanza en general, quiere proteger a las personas que alertan sobre ilícitos sistémicos de todo tipo. Hacerlo solo parcialmente sería una contradicción inexplicable o movida por intereses espurios.

No solo es preciso aumentar el ámbito material cuanto a las materias incluidas, sino también cuanto a las conductas: la Directiva prevé que estos sujetos informen sobre "infracciones", debiendo incluirse, para mayor protección y prevención, toda información relevante e indiciaria sobre hechos flagrantes, actuales, potenciales o presuntos que constituyan, sin limitarse a ellos, ilícitos, malas prácticas, abusos, irregularidades, mala gestión o fraude, amenazas graves y específicas, otras vulneraciones de leyes o normas o códigos éticos, contrarias o lesivas al interés general (<https://whistleblowingnetwork.org/News-Events/News/News-Archive/PRESS-RELEASE-Coalition-to-Make-Whistleblowing-Sa>), la justicia, la democracia, o contrarias a los objetivos y fines de las normas estatales y europeas, o daño, con independencia de que se hayan ya consumando, ejecutado, estén en fase de tentativa o se tenga indicios de que se van a producir, o que se produzcan, dentro o fuera del territorio del Estado con consecuencias en territorio nacional, tanto los sectores públicos como privados.

Por las mismas razones, para que esta legislación realmente sea un instrumento **para luchar contra la corrupción y los abusos sistémicos y no sea un mero trámite que mantiene la actual opacidad y déficit democrático**, se debe ampliar el sujeto a toda persona que pueda alertar contra un ilícito, siempre que este sea sistémico y no puntual. Es decir, las y los alertadores deben ser instrumentos al servicio del bien común. Para otro tipo de ilícito o delitos que no afectan al bien común general, existen ya infinidad de normas en nuestro ordenamiento jurídico.

Concretamente, en lo relacionado con esta pregunta, nuestra Proposición de Ley prevé lo siguiente:

Artículo 1.- Objeto.

1. Esta Ley tiene por objeto establecer medidas para la protección de las personas que revelen informaciones sobre posibles irregularidades, infracciones o acciones u omisiones que produzcan ilícitos o malas prácticas que sean contrarias o lesivas al interés general o contrarias a los objetivos y fines de las normas estatales y europeas, y que se hayan producido, se estén produciendo o sea probable que se produzcan en el

ámbito de las administraciones y sector público y empresas o entidades públicas y privadas. (...)

Artículo 4.- Informaciones que constituyen alerta.

1. Las informaciones objeto de alerta son las relativas al interés general tal y como definido en el punto 3.e) de la presente Ley que aporten información relevante e indiciaria sobre hechos flagrantes, actuales, potenciales o presuntos que constituyan, sin limitarse a ellos, ilícitos, malas prácticas, abusos, irregularidades, mala gestión o fraude, amenazas graves y específicas, otras vulneraciones de leyes o normas, o daño, con independencia de que se hayan ya consumando, ejecutado, estén en fase de tentativa o se tenga indicios de que se van a producir, o que se produzcan, dentro o fuera del territorio del Estado, en los siguientes ámbitos, sin limitarse a ellos:

a) La comisión de cualquier delito doloso, imprudente o negligente;

b) Cualquier vulneración de los derechos humanos, ataques contra las libertades fundamentales, vulneraciones de los derechos de los trabajadores, condiciones de sanidad y seguridad en el trabajo y otros derechos sociales, así como sobre el estado de derecho;

c) Accidentes, desastres, peligros naturales y otras emergencias;

d) Prácticas que entrañan riesgos para la vida y la salud de las personas o cualquier otra amenaza para la seguridad e integridad física, la salud pública, la seguridad de los productos de consumo, la seguridad del transporte, la seguridad alimentaria, la salud y seguridad animal, los derechos de los consumidores y usuarios, la seguridad nacional y mundial, la seguridad nuclear, la privacidad y la protección de datos personales, la seguridad de las comunicaciones electrónicas y sistemas de información, y el medio ambiente;

e) Malas prácticas administrativas o empresariales, en el seno de entidades públicas o privadas, relacionadas con el abuso de autoridad, los conflictos de interés, la corrupción, la malversación de caudales públicos, la prevaricación, el tráfico de influencias, el fraude fiscal, la responsabilidad y seguridad financiera, las infracciones de la libre competencia y normas relativas a las ayudas y subvenciones del Estado, así como infracciones relativas a servicios, productos y mercados financieros y a la prevención del blanqueo de capitales y financiamiento del terrorismo, entre otros;

f) Malas prácticas disciplinarias, administrativas, en materia de privacidad, protección de datos o cualquier otra negligencia u omisión por parte de las agencias gubernamentales, autoridades públicas o cualquiera de sus empleados, entidades legales, sus funcionarios y su personal, abuso de poder, abuso de autoridad, mala administración, conflictos de intereses, incumplimiento de obligaciones legales;

g) Actos para el encubrimiento de estas irregularidades;

h) Cualquier otra información no incluida en las secciones anteriores que revele daño o una amenaza para el interés público.

i) en cualquier caso podrán ser objeto de alerta las infracciones de las normas previstas en el anexo a la Directiva (UE) 2019/1937, de 23 de octubre de 2019, del Parlamento Europeo y del Consejo sobre la

En nuestra dilatada experiencia trabajando con alertadores sabemos que hay al menos un 15% de los casos no se da ningún tipo de relación laboral. En estos casos, por ejemplo, quién alerta puede ser alguien afectado por el ilícito, un investigador/periodista o un activista que consiga descubrir pruebas, como Ramsay Orta o Flexispy whistleblowers. **También son frecuentes los casos en los que es alguien que tiene relaciones personales con quienes participan en una trama (ejemplo: caso Pujol en España).**

Consideramos que, en la armonización conjunta y legalmente explícita de las competencias compartidas del espacio de libertad, seguridad y justicia entre la UE y los Estados miembros, cabe absolutamente incluir a toda la ciudadanía en la protección que merecen cuando alertan sobre ilícitos y esto todavía más habiendo observado que la protección de los periodistas y demás facilitadores de que la información llegue a la opinión pública es más laxa de lo deseable.

Nuestra experiencia desmiente absolutamente que cuando no exista el desequilibrio de poder relacionado con el trabajo, no hay necesidad de protección contra represalias.

Si bien en el ámbito del trabajo las represalias típicas son la "terminación anticipada del contrato de servicios o la pérdida del negocio", "la coacción, intimidación u hostigamiento, el boicot empresarial o los daños a su reputación" los sufren absolutamente todos los ciudadanos que alertan sobre ilícitos contra el interés general.

En conclusión, **consideramos que cualquier persona que se enfrenta a un riesgo de represalias por alertar sobre abusos debería disfrutar de una protección.** La gama de escenarios es amplia: empleados con sus empleadores (o personal superior), civiles con las autoridades y niños con adultos. Además, cualquier parte que facilite este diálogo también debería disfrutar de protección.

Entendemos la intención de acotar el alcance de la Directiva para no invadir ámbitos de luchas contra los ilícitos ya cubiertos por otras competencias o legislaciones específicas, pero entendemos que donde se debe acotar es afirmando con mayor claridad que la Directiva cubre únicamente ilícitos que afectan al interés general – no los ilícitos en sí -, no dejando desprotegidos una parte considerable de los potenciales alertadores.

- ¿En qué ámbitos o materias concretas la protección de los denunciantes necesita un mayor refuerzo?

Reiteramos que la protección de los alertadores no debe centrarse en un ámbito o materia concretos, sino que debe abarcar todas las posibilidades para dar una protección sin discriminación y sobre todo sin un injustificable "permiso para trasgredir" a ciertos ámbitos concretos, como podrían ser los partidos, la Casa Real o similares.

2. En relación con el ámbito de aplicación personal previsto en el artículo 4 de la Directiva:

- ¿Qué entidades del sector público deberían quedar integradas en el ámbito de aplicación personal de la Directiva?

Por lo anteriormente expuesto, **debe poderse alertar sobre las conductas arriba descritas en cualquier tipo de entidad, pública o privada.** En el ámbito de las administraciones públicas cuya actuación se rige por los principios de legalidad y de eficacia de los poderes públicos, así como en el de las empresas privadas cuyo tamaño o volumen de tráfico afectan a derechos e intereses de una gran parte de la sociedad en la que operan, la transparencia debe ser la norma y el secreto la excepción.

Concretamente, en lo relacionado con esta pregunta, nuestra Proposición de Ley prevé lo siguiente:

Artículo 3.- Definiciones y ámbito subjetivo de protección.

(...) e) Interés general: El ámbito de aplicación de esta ley se acota considerando interés general cualquier acto u omisión que ocurra, afecte o se lleve a cabo en o por parte de:

- 1) administraciones públicas y/o organizaciones administrativamente dependientes de la administración pública;*
- 2) cualquier persona física o jurídica cuya actuación afecte a más del 10% de la población de una circunscripción legal.*

- ¿Debe apostarse por una concepción amplia de sector público tomando como referencia el ámbito de aplicación subjetivo de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno? ¿Ha de incluirse órganos constitucionales y/o partidos políticos?

Como explicado anteriormente, **consideramos de vital importancia una concepción amplia del sector público, corrigiendo además las históricas lagunas de la Ley de Transparencia. Es importante incluir también los órganos constitucionales y los partidos políticos en el ámbito de aplicación personal de la transposición,** por ello, y como se verá en las preguntas que siguen, en la proposición de Ley registrada por Xnet se han incluido entre las entidades que deben disponer de canales internos de alerta.

EL HECHO DE QUE, POR PARTE DE QUIENES ESTÁ PROMOVRIENDO ESTA CONSULTA, SE INSINUE REDUCIR EL ALCANCE EN EL SECTOR PÚBLICO

Y QUE NO SE MENCIONE SINO DE FORMA AMBIGUA EL SECTOR PRIVADO, NOS PARECE DE EXTREMA GRAVEDAD.

3. En relación con la obligación de establecer canales y mecanismos de denuncia internos recogida en el artículo 8 de la Directiva:

- ¿Debe España acoger a la opción de denuncias anónimas?

Absolutamente sí, sino sería un paso atrás respecto a sus propios mecanismos de tutela del interés general.

Debe establecerse con claridad en la transposición de la Directiva que tanto la confidencialidad como el anonimato se erigen en derechos de la persona alertadora, solo con excepciones muy justificadas amparadas en la ley. En este sentido es muy importante el tema de la denominación de "alertadores" y no "denunciantes" que explicaremos más adelante.

La diferencia entre anonimato y confidencialidad es que el anonimato es el único que permite a la fuente de la información controlar en su totalidad su propia protección y el uso que se hace de la información. Si bien los derechos de confidencialidad deben reflejar los requisitos de mejores prácticas de la Directiva, en la práctica esas salvaguardias no han sido fiables, quedando ampliamente demostrada la vulnerabilidad y porosidad de los sistemas de alerta que se basan en la mera confidencialidad. Conlleva además peligros inherentes a que se centralice todo el poder (la información) en manos de unas pocas personas (directivos de corporaciones o superiores jerárquicos en las administraciones públicas). Es evidente que las corporaciones e instituciones deben cumplir sus deberes de transparencia e implementar sistemas de vigilancia de irregularidades e infracciones. Aun así, no es posible evitar abusos confiando en una suerte de autorregulación ya que el fraude y la corrupción se dan en posiciones privilegiadas respecto a tales sistemas internos. Por esto debemos aprovechar las oportunidades que ofrece ahora la tecnología y trazar cauces que nos permitan una vigilancia ciudadana distribuida. El uso de herramientas tecnológicas ahora permite ser más eficientes en la protección de la confidencialidad y anonimato de quien aporta información relevante. Esto permite corregir la mencionada asimetría. Debemos preservar el anonimato de las personas privadas porque son vulnerables cuando se exponen para proteger el bien común.

El anonimato es la más robusta protección que se le puede ofrecer a una o un ciudadano alertador y ya ha sido reconocido como cauce justo y necesario en España por la Fiscalía en sus recomendaciones desde 1993, así como **por diferentes disposiciones legales de nuestro ordenamiento y por organizaciones como la ONU** en su Report on Encryption, Anonymity, and The Human Rights Framework de 2015 (<http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/CallForSubmission.as>)

px). El anonimato es ya aceptado por las instituciones españolas, desde Fiscalía (https://www.fiscal.es/fiscal/PA_WebApp_SGNTJ_NFIS/descarga/instruccion03_1993.pdf?idFile=12794dc6-9acc-4da0-bbc1-daf779e2f084), a los Tribunales, a la CNMC, la Agencia Española de Protección de Datos o en los buzones anónimos para alertar sobre abusos que Xnet ha instalado en diversas instituciones como Oficinas Antifraude y Administraciones (<https://xnet-x.net/xnet-buzon-anonimo-generalitat-amb-fgc-lleida-terrasa-mollet-instituciones/>).

La “confidencialidad” no es suficiente. Del mismo modo lo pedía la Resolución del Parlamento Europeo, de 24 de octubre de 2017, sobre las medidas legítimas para la protección de los denunciantes (<http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P8-TA-2017-0402+0+DOC+XML+V0//ES>) que ha originado el borrador de Directiva. En el posicionamiento 49 dice: “Considera que la posibilidad de efectuar denuncias anónimas puede animar a los denunciantes a transmitir informaciones que en otras circunstancias no se habrían comunicado; (...) destaca que la identidad del denunciante, así como cualquier otra información que permita su identificación, no deben poder ser reveladas sin su consentimiento (...)”.

Concretamente, en lo relacionado con esta pregunta, nuestra Proposición de Ley prevé lo siguiente:

Artículo 2.- Ámbito subjetivo de aplicación.

1. Las siguientes administraciones y entidades legales deben establecer canales de alerta anónimos y seguros, internos y externos, cumpliendo con las obligaciones establecidas en el Título III: (...)

Artículo 7.- Derecho a la confidencialidad y al anonimato de la y el alertador y facilitador.

1. Los poderes públicos garantizarán el derecho de la o el alertador y facilitador a la confidencialidad y a la preservación de su anonimato si esta es la opción que elige la o el alertador o facilitador, y que su identidad no será revelada sin su consentimiento explícito a nadie. Este derecho también es aplicable a otros datos e información de la que pueda deducirse la identidad de la y el alertador o facilitador de manera directa o indirecta. Si es necesario por razones no discrecionales, como una orden judicial, revelar la identidad o la información de identificación de la o el alertador, o si esa información se revela por error, la autoridad pública lo notificará inmediatamente a la o el alertador. El error será severamente sancionado de acuerdo con los artículos 37 y 38 de la presente ley.

2. Las y los facilitadores y cualesquiera otras personas, públicas o privadas, a las que la o el alertador haya comunicado su identidad haciendo constar su voluntad de mantener su anonimato, están igualmente obligados a preservarlo y no pueden revelar la identidad de la o el alertador en ningún caso.

3. Los canales de recepción de alertas salvaguardarán estos derechos en los términos que disponen los artículos 14 y siguientes.

4. Las y los alertadores podrán comunicar al canal receptor la información de forma confidencial, esto es, dando a conocer su identidad pero

haciendo constar su voluntad de no divulgarla sin su consentimiento expreso o dejando posible la trazabilidad de su identidad (proporcionando información de la que pueda deducirse, por ejemplo, dejando visible su IP o no utilizando un canal anónimo y seguro). En este caso, sus datos personales o cualquier otra información que permita conocer la identidad de la o el alertador, no podrá ser divulgada por el personal autorizado que tramite la alerta sin su consentimiento expreso. Todo el personal autorizado o que tenga acceso a la información recibida mediante un canal de recepción de alertas, incluso de forma no autorizada o incidental, quedará obligado en los términos previstos en el presente artículo y a las responsabilidades derivadas de la comisión de los delitos tipificados como descubrimiento y revelación de secretos.

5. Exceptuando lo indicado en el apartado primero del presente artículo, solo la o el alertador podrá decidir sobre una eventual renuncia al anonimato y/o confidencialidad, que podrá producirse en cualquier momento del procedimiento.

6. Si con posterioridad a la alerta se identifica a una o un alertador anónimo, gozará de protección en virtud de la presente Ley.

Artículo 9.- Derecho al asesoramiento y defensa jurídica.

(...) 4. Las y los alertadores y facilitadores ostentan la condición de interesados en cuantos procedimientos traigan causa de la comunicación de información que hayan efectuado, por lo tanto siendo objeto de protección de acuerdo con la presente Ley en todas las investigaciones y otros procedimientos resultantes de la alerta. Estos procedimientos tendrán carácter contradictorio, garantizando en su caso el anonimato o confidencialidad de la identidad de la o el alertador. (...)

Artículo 14.- Protección de la confidencialidad o anonimato.

1. Los canales de recepción de alertas deberán estar dotados de mecanismos que permitan proteger la confidencialidad o anonimato de las y los alertadores y facilitadores.

2. La información sobre el acceso al canal de comunicación, el modo y los límites de la preservación del anonimato que ofrece, deben ser explicitados detalladamente, para que la y el alertador tenga toda la información necesaria y no pueda ser inducido a error por omisión de información o por no cumplir los requisitos informativos requeridos por el presente artículo y el artículo 16.

Esta información deberá ser proporcionada por la o el administrador del canal de recepción de alertas de forma concisa, leal, transparente, inteligible y de fácil acceso y entendimiento, con un lenguaje claro y sencillo, facilitándose por escrito o por otros medios, inclusive, por medios electrónicos.

La o el administrador del canal de recepción de alertas, habida cuenta de las circunstancias y del contexto específico en que se produzca la alerta, facilitará a la y al alertador cuanta información complementaria sea necesaria para garantizar la protección de la confidencialidad de sus datos y de la alerta o anonimato.

3. A estos efectos solo se considerarán anónimos y seguros aquellos buzones, como líneas telefónicas o mecanismos de comunicación

electrónica que garanticen su acceso a través de navegación y conexión anónimas. Los buzones deberán informar con indicaciones previas claras y sencillas sobre cómo utilizarlos sin exponer la propia identidad – incluyendo la “identidad electrónica” (Internet Protocol o IP) – y sobre las formas de eliminación de los metadatos para que los documentos no comprometan la anonimidad del alertador. Deberán proveer a la y al alertador de acuse de recibo con código identificador, u otro procedimiento seguro, que permita el seguimiento de las actuaciones y las comunicaciones sucesivas con el alertador sin perjudicar su anonimato. Las administraciones o entes responsables del canal aplicarán las medidas técnicas y organizativas adecuadas para la protección de los datos cuando se recaben, se transmitan o se conserven.

4. Los canales que no reúnan las condiciones del apartado anterior no podrán publicitarse como anónimos y seguros, pudiendo ser, en caso contrario, objeto de sanción por afectar al derecho a la indemnidad de la y el alertador. También podrán ser objeto de sanción aquellos canales que siendo solamente confidenciales no informen de este hecho, debiendo informar en todo momento de que no se trata de un canal anónimo y seguro.

5. En todo caso deberá respetarse el derecho a la confidencialidad y al anonimato previsto en el artículo 7.

Tal y como indicamos en nuestra Proposición (<https://xnet-x.net/proposicion-ley-proteccion-integral-alertadores/>), “existe una situación de asimetría de fuerzas entre los ciudadanos y las instituciones o las corporaciones que imposibilita de facto que las personas puedan cumplir con el deber ciudadano de denunciar los delitos de los que tengan conocimiento, así como alertar sobre comportamientos impropios, irregularidades o actividades ilícitas.

Las innovaciones tecnológicas, disminuyendo considerablemente el riesgo de comprometer la identidad de quien alerta, contribuyen, con toda seguridad, al objetivo de esta directiva y a una mayor eficacia en la lucha contra el fraude. Deben integrarse de forma explícita y positiva, aunque sin ingenuidades – siempre que hay humanos pueden haber abusos.

Ya existen legislaciones contra las denuncias falsas que se pueden mencionar explícitamente de acuerdo con la Recomendación del Consejo de Europa (10): «Los Estados miembros establecerán sanciones efectivas, proporcionadas y disuasorias aplicables a las personas que hagan revelaciones falsas, manteniendo la protección y aplicando las normas de la legislación general». **Medidas contra alertas falsas ya han sido previstas tanto en la Directiva como en nuestra proposición de Ley:**

Artículo 13.- De la responsabilidad de la y el alertador y facilitador.

1. La y el alertador y el facilitador deben únicamente tener una convicción razonable en la verosimilitud y fiabilidad de la información que comuniquen, que, como indicado en el artículo 4.1 debe ser información relevante e indiciaria. La responsabilidad de la comprobación de los hechos objeto de la alerta, de determinar si hay suficiente información para investigar las posibles infracciones y de la cualificación de los

mismos como posibles delitos o acciones contra el interés general recae, en todo caso, sobre el organismo o institución a cargo de la investigación.

2. Cuando la resolución que ponga término a la averiguación de los hechos generados por la alerta concluya que no se trate de irregularidades, infracciones, malas prácticas o hechos constitutivos de ilícito penal, la y el alertador o facilitador mantendrá la protección reconocida por la presente Ley y no sufrirá perjuicio, sanción, o represalia alguna, a menos que se pruebe que la persona conocía la falsedad de la información en el momento de la alerta e informó deliberadamente sobre la misma.

3. Con la misma excepción señalada en el apartado anterior, la y el alertador y el facilitador no serán responsables por los daños y perjuicios que puedan derivarse de la comunicación o divulgación de la alerta o de las acciones realizadas para revelar la información, ni incurrirán en ningún otro tipo de responsabilidad, ya sea disciplinaria, civil o penal, que pueda derivar de tales circunstancias, incluidas expresamente las concernientes al posible menoscabo del derecho al honor, de los derechos de autor, de los secretos, secretos comerciales, prevención de blanqueo de capitales y de la protección de datos personales.

4. A la y al alertador y/o facilitador que hubiesen sido partícipes en los hechos objeto de la información constitutiva de alerta les será de aplicación la 7ª atenuante cualificada prevista por el artículo 21.7ª del Código Penal, para que la pena a la que podrían ser condenados sea la inferior en uno o dos grados.

- ¿Deben las denuncias anónimas reconocerse tanto en el sector público como en el privado?

Sí. Siguiendo el razonamiento de la pregunta anterior, **no debe haber distinciones en este sentido entre sector público y privado** cuyos actos, actuaciones o productos alcancen más del 10% de la población de una circunscripción legal.

- ¿Qué sujetos deberían cumplir con la obligación de establecer canales y/o mecanismos de denuncia interna?

Concretamente, en lo relacionado con esta pregunta, nuestra Proposición de Ley prevé lo siguiente:

Artículo 2.- Ámbito subjetivo de aplicación.

1. Las siguientes administraciones y entidades legales deben establecer canales de alerta anónimos y seguros, internos y externos, cumpliendo con las obligaciones establecidas en el Título III:

a) La Administración General del Estado, las Administraciones de las Comunidades Autónomas y de las Ciudades de Ceuta y Melilla.

b) Las entidades gestoras y los servicios comunes de la Seguridad Social así como las mutuas de accidentes de trabajo y enfermedades profesionales colaboradoras de la Seguridad Social.

c) Entidades de derecho público con personalidad jurídica propia de ámbito nacional y autonómico, los organismos autónomos, las Agencias Estatales y las entidades de Derecho Público que, con independencia funcional o con una especial autonomía reconocida por la Ley, tengan atribuidas funciones de regulación o supervisión de carácter externo sobre un determinado sector o actividad, incluyendo Autoridades Independientes.

d) El Defensor del Pueblo e instituciones autonómicas análogas.

e) El Consejo General del Poder Judicial y la Fiscalía General del Estado.

2. Las siguientes entidades deben establecer canales de alerta internos que cumplan con las obligaciones establecidas en el Título III:

a) Los partidos políticos, las organizaciones sindicales y las organizaciones empresariales.

b) Las sociedades mercantiles en cuyo capital social la participación, directa o indirecta, de las entidades previstas en este artículo sea superior al 50 por 100; las fundaciones y las asociaciones constituidas por las administraciones, organismos y entidades previstas en este artículo.

c) Administraciones del Estado, Autonómicas, Provinciales y Municipios con más de 10,000 residentes no incluidas en el apartado anterior, y en todo caso, la Casa de su Majestad el Rey, el Congreso de los Diputados, el Senado, el Tribunal Constitucional, así como el Banco de España, el Consejo de Estado, el Tribunal de Cuentas, el Consejo Económico y Social y las instituciones autonómicas análogas.

d) Entidades privadas con más de 50 trabajadores o de cualquier envergadura cuando operen en materia de servicios financieros u otras materias con riesgo de blanqueo de capitales.

e) Universidades.

3. Las Administraciones Públicas y las entidades jurídicas no incluidas en secciones anteriores, tanto en el sector público como privado, deben cumplir y respetar los derechos y obligaciones establecidos en la presente Ley para proteger alertadores y facilitadores.

4. Cualquier otra administración o entidad, pública o privada, incluyendo, pero sin limitarse a, los medios de comunicación, organizaciones no gubernamentales, organizaciones sindicales, miembros del poder legislativo, organizaciones y asociaciones profesionales, podrán establecer canales externos de alerta.

No solo debe preverse la obligación para algunos y la libertad para otros de establecer canales de alerta, sino también unos mínimos estándares para establecerlos, guardando la seguridad de los intervinientes y de la información. Por ello, **es imprescindible que las condiciones y requisitos que la regulación de los sistemas de información o canales de recepción de alertas de que dispondrán las y los alertadores deba contenerse en la transposición de la Directiva y no remitirse a la vía reglamentaria**, debiendo prever, entre otros aspectos: los sujetos obligados a implantarlos, los ritmos en la implantación de sistemas internos de alerta en corporaciones y entidades públicas y privadas, las condiciones de anonimato y confidencialidad pertinentes,

las condiciones sobre la gestión de los canales (independencia, imparcialidad, seguridad, mediante recursos internos, externos o compartidos), de información sobre dichos canales que debe proporcionarse, sobre las protecciones y riesgos derivados de su uso, las infracciones y sanciones por el incumplimiento de los requisitos previstos por la ley en su implantación, los procedimientos de seguimiento de las alertas, etc.

LA IMPORTANCIA DE LA LIBERTAD DE ELECCIÓN DEL CANAL PARA ALERTAR

Es fundamental y no eludible para no dejar sin valor el propio espíritu de la ley, dejar a la o el alertador la libertad de elección de elegir el canal de alerta que considere. Donde hay que aplicar rigor es a estos canales y no limitar esta elección.

Deben existir canales internos, pero no deben ser de uso obligado porque esta obligación llegaría a contradecir el propio ordenamiento jurídico vigente: quien sea testigo de un delito debe poder denunciarlo. Deben existir canales externos tanto institucionales como no institucionales (de ONGs, entidades y medios de comunicación), **para garantizar la pluralidad de opciones y de este modo la optimización de los tiempos de actuación.**

No hay ninguna duda en España que esto tiene que ser así: la gran mayoría de casos de corrupción se han podido encarar cuando se han usado canales que no son los institucionales.

Es fundamental y no eludible para no dejar sin valor el propio espíritu de la ley, dejar a la o el alertador la libertad de elección de elegir el canal de alerta que considere. Donde hay que aplicar rigor es a estos canales y no limitar esta elección.

La o el alertador debe poder decidir cuál es el canal más seguro para alertar: canal interno, externo o difusión pública. No permitir que sea quien quiera alertar quien determine el canal de alerta más apropiado, puede desactivar gran parte de la utilidad de la directiva.

En nuestra dilatada experiencia, la mayoría de los alertadores que han usado canales internos de la entidad que querían sacar a la luz abusos, solo han conseguido la destrucción de pruebas y mucho sufrimiento para ellos y sus familias.

Pedir u obligar a que primero se alerte internamente, obligando al alertador a tener que demostrar que tiene muy buenos motivos para no hacerlo, en buena parte desactiva los objetivos de la Directiva y desincentiva a los posibles alertadores y facilitadores. En una gran mayoría de los casos, el alertador no estaría amparado: piensen en Snowden o en el caso Luxleaks entre infinidad de otros. Entendemos que el motivo es el de evitar inútiles efectos negativos para la reputación de una empresa y/o institución, pero, por ejemplo, en los casos anteriormente mencionados, no hubiera sido una solución.

No podemos aceptar esta restricción si no es acotada de forma extremadamente razonable, ya que **un solo caso de ineficiencia de un canal interno debería ser suficiente motivo por no usarlo**. Ser tajantes con esto tendría el efecto de obligar a las entidades a tener canales internos realmente eficaces y sería la única manera para legitimar que se deba usarlos en primera instancia.

La posibilidad de utilizar canales externos o de revelar públicamente la información en primera instancia debe ser clara, sobre todo cuando "(...) no puede esperarse razonablemente que los canales internos funcionen adecuadamente. Este es el caso, en particular, cuando los denunciantes tengan razones válidas para pensar que podrían sufrir represalias en relación con la alerta sobre infracciones, en particular como resultado de una vulneración de su confidencialidad, y que las autoridades competentes estarían mejor situadas para adoptar medidas eficaces para ocuparse de la infracción. Las autoridades competentes podrían estar mejor situadas, por ejemplo, cuando el responsable último en el contexto laboral está implicado en la infracción, o existe el riesgo de que se oculten o destruyan la infracción o las pruebas conexas o, de manera más general, porque la eficacia de las investigaciones por parte de las autoridades competentes podría verse amenazada de otra manera, como en el caso de que se denuncien prácticas colusorias u otras infracciones de las normas en materia de competencia; o porque la infracción requiere medidas urgentes, por ejemplo, para proteger la vida, la salud y la seguridad de las personas o para proteger el medio ambiente. (...)" (Considerando 62 de la Directiva).

En Estados muy corruptos, no hay otro modo que hacer pública la información para que personas poderosas no aplasten la verdad cuando operan contra el interés general.

Consideramos que las legítimas consideraciones sobre los riesgos reputacionales deben trasladarse a la responsabilidad en la forma de publicar y en los códigos deontológicos y legales del periodismo, no en el alertador. El cumplimiento de esta salvaguarda será responsabilidad de quien realice la publicación. Así lo indicamos en el artículo 4.2.a) de nuestra Proposición de Ley.

La alerta sobre irregularidades en el interés público es una forma de libertad de expresión protegida, como confirma la jurisprudencia del Tribunal Europeo de Derechos Humanos en virtud del artículo 10 del Convenio Europeo de Derechos Humanos, del que todos los países de la UE son parte: "las personas que informan sobre amenazas o daños al interés público (...) hacen uso de su derecho a la libertad de expresión. El derecho a la libertad de expresión es consagrado en el artículo 11 de la Carta de los Derechos Fundamentales de la Unión Europea y en el artículo 10 de la Convención Europea de Derechos Humanos (CEDH) y abarca la libertad y el pluralismo de los medios". Creemos firmemente que toda la ciudadanía se merece el mismo trato y protección porque sino se contradeciría incluso los tratados europeos que garantizan los derechos y libertades de la población. El artículo 11 de la Carta de los Derechos Fundamentales de la Unión Europea dice expresamente "Todos tienen derecho a la libertad de expresión. Este derecho incluirá la libertad de

mantener opiniones y de recibir e impartir información e ideas sin interferencia de la autoridad pública e independientemente de las fronteras".

Las revelaciones públicas son esenciales para el establecimiento de un sistema horizontal que brinde alternativas seguras a las personas alertadoras y facilitadoras. Esta opción debe ser incluida en la transposición de la Directiva, quien las prevé en su artículo 19, tanto para la protección de alertadores y facilitadores como para la defensa de derechos fundamentales como el acceso a la información y la libertad de expresión.

Concretamente, en lo relacionado con estas cuestiones, nuestra Proposición de Ley prevé lo siguiente:

Artículo 3.- Definiciones y ámbito subjetivo de protección.

A los efectos de esta Ley se entiende por: (...)

c) Canales de recepción de alertas (denuncias-señalamientos específicos llevados a cabo por un o una alertadora): son sistemas o mecanismos de comunicación y recepción de alertas, definidos y regulados en el Título III de la presente ley, que se ponen a disposición de cualquier persona que posea información que pueda constituir una alerta. Estos canales pueden ser internos, cuando son establecidos por la propia administración o entidad pública o privada para las alertas referidas a su funcionamiento y ámbito de actuación, o bien externos, cuando son canales habilitados por cualquier administración, entidad o plataforma para la comunicación y recepción de alertas de cualquier ámbito de actuación.

El hecho de que se habiliten estos canales no inhabilita la protección a las y los alertadores que no los hayan utilizado para revelar, notificar o divulgar una información constitutiva de alerta, como, por ejemplo, las alertas a supervisores o superiores, cuando se alerte cumpliendo con deberes profesionales o se alerte ante una o un facilitador o ante cualquier persona que pueda proporcionar información relevante, investigar o tomar medidas sobre la supuesta conducta impropia.

d) Divulgación pública: consiste en hacer accesible al público la información que constituye una alerta. (...)

TÍTULO III. SISTEMAS DE INFORMACIÓN O CANALES DE RECEPCIÓN DE ALERTAS

Artículo 14.- Protección de la confidencialidad o anonimato.

1. Los canales de recepción de alertas deberán estar dotados de mecanismos que permitan proteger la confidencialidad o anonimato de las y los alertadores y facilitadores.

2. La información sobre el acceso al canal de comunicación, el modo y los límites de la preservación del anonimato que ofrece, deben ser explicitados detalladamente, para que la y el alertador tenga toda la información necesaria y no pueda ser inducido a error por omisión de información o por no cumplir los requisitos informativos requeridos por el presente artículo y el artículo 16.

Esta información deberá ser proporcionada por la o el administrador del canal de recepción de alertas de forma concisa, leal, transparente, inteligible y de fácil acceso y entendimiento, con un lenguaje claro y

sencillo, facilitándose por escrito o por otros medios, inclusive, por medios electrónicos.

La o el administrador del canal de recepción de alertas, habida cuenta de las circunstancias y del contexto específico en que se produzca la alerta, facilitará a la y al alertador cuanta información complementaria sea necesaria para garantizar la protección de la confidencialidad de sus datos y de la alerta o anonimato.

3. A estos efectos solo se considerarán anónimos y seguros aquellos buzones, como líneas telefónicas o mecanismos de comunicación electrónica que garanticen su acceso a través de navegación y conexión anónimas. Los buzones deberán informar con indicaciones previas claras y sencillas sobre cómo utilizarlos sin exponer la propia identidad – incluyendo la “identidad electrónica” (Internet Protocol o IP) – y sobre las formas de eliminación de los metadatos para que los documentos no comprometan la anonimidad del alertador. Deberán proveer a la y al alertador de acuse de recibo con código identificador, u otro procedimiento seguro, que permita el seguimiento de las actuaciones y las comunicaciones sucesivas con el alertador sin perjudicar su anonimato. Las administraciones o entes responsables del canal aplicarán las medidas técnicas y organizativas adecuadas para la protección de los datos cuando se recaben, se transmitan o se conserven.

4. Los canales que no reúnan las condiciones del apartado anterior no podrán publicitarse como anónimos y seguros, pudiendo ser, en caso contrario, objeto de sanción por afectar al derecho a la indemnidad de la y el alertador. También podrán ser objeto de sanción aquellos canales que siendo solamente confidenciales no informen de este hecho, debiendo informar en todo momento de que no se trata de un canal anónimo y seguro.

5. En todo caso deberá respetarse el derecho a la confidencialidad y al anonimato previsto en el artículo 7.

Artículo 15.- Otros tipos de canales

El canal de recepción de alertas establecido por las entidades, cumpliendo las características del apartado tercero del artículo anterior, debe permitir comunicaciones escritas y/o orales y puede establecerse por los siguientes medios:

- a) Vía correo postal*
- b) Vía buzones físicos de queja*
- c) Vía una plataforma online (a través de la intranet de la entidad o de internet)*
- d) Vía telefónica u otros sistemas de mensajería de voz.*

Artículo 16.- Información sobre los canales de comunicación y recepción de alertas

Las entidades que administren canales de recepción de alertas deberán publicar de forma concisa, leal, transparente, inteligible y de fácil acceso y entendimiento, con un lenguaje claro y sencillo, en un apartado separado, identificable y accesible de sus páginas web, como mínimo, la información siguiente:

a) Las condiciones bajo las cuales las y los alertadores y facilitadores gozarán de protección.

b) Los datos de contacto de los canales, previstos en el artículo anterior, proporcionados por la entidad pública o privada, y si se trata de un canal anónimo y seguro que cumple con los requisitos del artículo 14.3, o cuando no sea el caso que sólo garantiza la obligatoria confidencialidad debe advertir de los posibles riesgos que esto puede conllevar en el uso del canal para la y el alertador en caso de alertar.

c) Los procedimientos aplicables a las alertas, incluyendo la manera como la entidad puede solicitar a la y al alertador y/o facilitador la clarificación de la información proporcionada o solicitar información adicional, los plazos en que se informará al mismo del seguimiento de la alerta, el tipo de contenido de estas comunicaciones y los posibles recursos contra las mismas.

d) El régimen de confidencialidad y protección de datos personales aplicables a la alerta.

e) La naturaleza del seguimiento que se dará a la alerta.

f) Las sanciones y procedimientos disponibles contra posibles represalias y la posibilidad de recibir consejo y asesoramiento confidenciales para las personas que estén considerando alertar sobre un hecho o información.

g) Una declaración que explique claramente las condiciones bajo las cuales las y los alertadores no incurrirán en responsabilidad conforme al artículo 4 de la presente Ley.

h) Las y los administradores de los canales de recepción de alertas deberán poder prestar asesoramiento previo sobre el contenido de la presente Ley a quienes pretendan informar, en condición de alertador o facilitador, sobre un hecho constitutivo de alerta.

2. Las y los administradores de los canales de recepción de alertas deberán poder prestar asesoramiento previo sobre el contenido de la presente Ley a quienes pretendan informar, en condición de alertador o facilitador, sobre un hecho constitutivo de alerta, incluyendo información sobre las condiciones y procedimientos de alerta ante las autoridades competentes y, cuando fuere necesario, ante instituciones, entidades, oficinas o agencias de la Unión Europea.

3. La entidad responsable del canal de alerta informará, sin constituir esta una lista exhaustiva, sus empleados, proveedores, personal temporal, y usuarios o clientes de la existencia del canal o canales de alerta, junto con la información prevista en los apartados anteriores.

Esta información puede publicarse en un lugar visible y accesible, y puede proporcionarse a través de la página web de la entidad, pudiendo incluso proporcionarse mediante cursos de formación del personal.

Artículo 17.- Procedimiento de alerta

El procedimiento de alerta y de seguimiento de las alertas debe incluir y garantizar el cumplimiento de los siguientes aspectos:

a) *El mantenimiento de la confidencialidad sobre la identidad de la y el alertador, o en su caso su anonimidad conforme al artículo 7, y de las personas involucradas en la información proporcionada por éste, además del resto de información proporcionada por la o el alertador, tomando las*

medidas necesarias y evitando el acceso a dicha información por personal no autorizado.

b) El canal de recepción de alertas deberá permitir el almacenamiento durable de la información, conforme al artículo 21, para permitir futuras investigaciones.

c) La autonomía del canal externo de alerta que pueda o deba haberse establecido en la entidad respecto al canal interno de alerta.

d) La oportunidad de la y el alertador de responder a la negación de las presuntas irregularidades de que alertó.

e) El acuse de recibo de la alerta, que deberá remitirse en un plazo máximo de 7 días desde su recepción si la alerta incluía los datos de contacto del alertador o facilitador.

- I) Tras el análisis de la información proporcionada por la y el alertador y/o facilitador, mediante declaración-adjunta al acuse de recibo, la entidad deberá comunicar a la y al alertador y/o facilitador:*
 - - Si considera que hay suficiente información para una mayor investigación;*
 - - O que la misma no incluye información relevante o indicios consistentes sobre la infracción por lo que se considera la alerta cerrada. La y el alertador tendrá derecho a responder dicha determinación preliminar.*
 - En el caso que la y el alertador o facilitador no esté de acuerdo con la decisión de la o el administrador del canal, podrá recurrir ante la Autoridad Independiente de Protección de las y los Alertadores y Facilitadores o ante la Jurisdicción competente.*
- II) En caso de que una entidad no sea capaz de analizar y valorar la información recibida a efectos de emitir la declaración constitutiva anterior, por la voluminosidad de la información proporcionada, la entidad puede pedir el consentimiento del alertador y/o facilitador para trasladar la alerta a la Autoridad Independiente de Protección de los Alertadores y Facilitadores para que la misma proceda a realizar su seguimiento.*
- No podrán trasladar la información presuntamente constitutiva de alerta a la Autoridad, los Juzgados, Tribunales, Ministerio Fiscal y Fuerzas y Cuerpos de seguridad del Estado, quienes deberán en todo caso investigar la información constitutiva de alerta.*

f) En su caso, la designación de uno, varios miembros del personal, un departamento o un tercero, que en todo caso deberá ser imparcial, como encargado de la recepción de las alertas, denominado administrador del canal.

- I) En los canales de recepción de alertas que se operen por terceras entidades autorizadas a recibir alertas por parte de entidades públicas y privadas, deberán respetarse los principios de independencia, confidencialidad, protección de datos personales y secreto, además de los requisitos informativos mencionados en el artículo 16.*
- II) La o el administrador del canal se encargará de hacer un seguimiento diligente de la alerta, mantener la comunicación con la y el alertador, y en caso de ser preciso, solicitar información*

adicional y mantener a la y al alertador informado del procedimiento seguido tras su alerta.

- *Con el consentimiento de la y el alertador, las y los administradores del canal serán responsables de remitir la información constitutiva de alerta a las instituciones competentes para que sea objeto de investigación.*
- *III) Como prerequisite, la o el administrador o administradores del canal deberán recibir formación profesional específica para gestionar canales de alerta.*
- *IV) Todas las actividades del personal para cumplir con las responsabilidades que conllevan los canales de alerta estarán protegidas bajo esta Ley.*

g) Las y los administradores de los canales de recepción de alertas deberán asegurarse que en caso de recibir una alerta a través de otros canales o por miembros del personal distintos a los encargados de su recepción, estos remitirán la alerta a los encargados preservando la confidencialidad de la información y sin modificar su contenido.

Artículo 18.- Libertad de elección.

Aunque se establece la obligación por parte de los poderes públicos de fomentar el uso de canales internos como primera opción para la comunicación de alertas, asegurándose de que estos ofrezcan todas las garantías de fiabilidad, seguridad, independencia y eficacia en la detección y resolución efectiva y duradera de ilícitos y abusos y en la protección de las y los alertadores eliminando todo riesgo de represalia, es libre la decisión del alertador de elección del canal más adecuado para su comunicación, sin tener que acudir preceptivamente a ningún canal específico ni tener que justificar su elección, y sin que esto suponga limitación alguna de los derechos y garantías que le asisten en esta Ley.

La o el alertador no está obligado a comunicarse a través de un canal interno de alerta, y retiene todos los derechos de esta Ley para revelar información protegida a un supervisor o superior, como parte de sus deberes profesionales, a una Autoridad, a otro testigo que pueda tener información relevante para apoyar la información, o a cualquier facilitador o facilitadora tal y como definido en el artículo 3.b) de la presente ley.

Artículo 19.- Sistemas internos.

1. Deberá informarse, en un plazo no superior a 3 meses desde el acuse de recibo, y cada tres meses, sobre el seguimiento realizado de la alerta y en todo caso de su resultado. En el caso de no haber enviado un acuse de recibo, este plazo empezará a correr en el momento de la expiración del plazo para emitirlo. La y el alertador tendrá derecho a presentar observaciones, que deberán incluirse en el informe final, sobre la exhaustividad y razonabilidad de la resolución de la alerta.

La comunicación sobre el resultado no debe afectar las normas europeas que incluyen posibles restricciones en la publicación de decisiones en el ámbito financiero y tributario.

2. Las entidades privadas con más de 50 trabajadores y menos de 249 podrán compartir recursos para la recepción e investigación de las alertas, sin perjuicio del cumplimiento de las obligaciones de confidencialidad, información del procedimiento a la y al alertador y abordar el incumplimiento detectado. Los canales de recepción de alertas podrán ser compartidos entre municipios o por uniones de municipios siempre que se garantice que la información recibida y dirigida sólo a uno de ellos no es accesible por los otros.-

Artículo 20.- Sistemas externos.

1. Deberá informarse, en un plazo no superior a 3 meses desde el acuse de recibo, y cada tres meses, sobre el seguimiento realizado de la alerta y en todo caso de su resultado. En el caso de no haber enviado un acuse de recibo, este plazo empezará a correr en el momento de la expiración del plazo para emitirlo. La y el alertador tendrá derecho a presentar observaciones, que deberán incluirse en el informe final, sobre la exhaustividad y razonabilidad de la resolución de la alerta. La comunicación sobre el resultado no debe afectar las normas europeas que incluyen posibles restricciones en la publicación de decisiones en el ámbito financiero y tributario.

2. En caso de gran afluencia de alertas, las y los administradores de los canales de recepción de alertas podrán priorizar aquellas que informen sobre infracciones de disposiciones esenciales que se encuentren dentro del ámbito de aplicación de la Ley o aquellas que sean susceptibles de afectar más gravemente el interés público, sin perjuicio del cumplimiento de los límites temporales establecidos en el artículo 17 y el presente artículo.

3. Cualquier entidad responsable de un canal externo de recepción de alertas que reciba una alerta a la que no pueda dar seguimiento por no disponer de las competencias necesarias, la remitirá a la autoridad competente sin demora.

4. Las entidades que administren canales externos de alerta deberán revisar los procedimientos establecidos de acuerdo con el presente capítulo regularmente y como mínimo una vez cada tres años. En esta revisión deberán tener en cuenta la experiencia adquirida por ellas y por otras entidades y autoridades y adaptar sus procedimientos de acuerdo con la misma.

Artículo 21.- Almacenamiento de la información constitutiva de alerta

1. Las y los administradores de canales de recepción de alertas, tanto internos como externos, deberán almacenar de forma segura todas las alertas para asegurar que las mismas son accesibles y que la información que contienen puede utilizarse para aplicar las medidas coercitivas o de cumplimiento necesarias. Deberán almacenarse por el tiempo estrictamente necesario y proporcionado, conservando en todo caso su confidencialidad y garantizando el acceso sólo al personal autorizado.

2. Cuando el canal de alerta consista en una línea telefónica u de mensajería de voz, las y los administradores de dicho canal, con el consentimiento de la y el alertador, podrán documentar la alerta grabando la conversación en formato durable y accesible o mediante la transcripción

de la conversación realizada por el personal encargado de recibir las alertas. En este último caso, debe ofrecerse a la y al alertador la posibilidad de verificar, rectificar y aceptar la transcripción de la llamada, si así lo desea, firmarla.

Cuando el canal de recepción de alertas proporcionado consista en un medio telefónico o de mensajería de voz que no permita la grabación, el personal de la y el administrador del canal podrá documentar la alerta indicando precisamente los minutos de duración de la conversación, debiendo ofrecer a la y al alertador la posibilidad de verificar, rectificar y aceptar el acta de la alerta.

3. Cuando la o el alertador solicite reunirse personalmente con un miembro del personal de la y el administrador del canal de recepción de alertas, la y el administrador deberá asegurar, bajo el consentimiento de la y el alertador, que se almacenarán los registros precisos y completos sobre la reunión en un soporte durable y accesible, pudiendo documentarla mediante una grabación de la conversación o mediante anotación y minutaje, por parte del personal de la y el administrador, debiendo ofrecer a la y al alertador la posibilidad de verificar, rectificar y aceptar el acta de la alerta.

- ¿Debe España asegurarse que las entidades privadas de menos de 50 trabajadores establezcan mecanismos y/o canales de denuncia internos?

Concretamente, en lo relacionado con esta pregunta, nuestra Proposición de Ley prevé lo siguiente:

Artículo 2.- Ámbito subjetivo de aplicación.

(...) 2. Las siguientes entidades deben establecer canales de alerta internos que cumplan con las obligaciones establecidas en el Título III:

(...) b) Las sociedades mercantiles en cuyo capital social la participación, directa o indirecta, de las entidades previstas en este artículo sea superior al 50 por 100; las fundaciones y las asociaciones constituidas por las administraciones, organismos y entidades previstas en este artículo.

(...) d) Entidades privadas con más de 50 trabajadores o de cualquier envergadura cuando operen en materia de servicios financieros u otras materias con riesgo de blanqueo de capitales.

(...) 3. Las Administraciones Públicas y las entidades jurídicas no incluidas en secciones anteriores, tanto en el sector público como privado, deben cumplir y respetar los derechos y obligaciones establecidos en la presente Ley para proteger alertadores y facilitadores.

4. Cualquier otra administración o entidad, pública o privada, incluyendo, pero sin limitarse a, los medios de comunicación, organizaciones no gubernamentales, organizaciones sindicales, miembros del poder legislativo, organizaciones y asociaciones profesionales, podrán establecer canales externos de alerta.

Artículo 19.- Sistemas internos.

(...) 2. Las entidades privadas con más de 50 trabajadores y menos de 249 podrán compartir recursos para la recepción e investigación de las alertas, sin perjuicio del cumplimiento de las obligaciones de confidencialidad, información del procedimiento a la y al alertador y abordar el incumplimiento detectado. Los canales de recepción de alertas podrán ser compartidos entre municipios o por uniones de municipios siempre que se garantice que la información recibida y dirigida sólo a uno de ellos no es accesible por los otros.

En un ejercicio de ponderación de las capacidades de las entidades consideradas pequeñas con la protección del interés general, creemos que **no sería proporcional obligar al establecimiento de estos canales, con todas las obligaciones y responsabilidades derivadas de ello, a entidades demasiado pequeñas cuando existan multiplicidad de canales externos accesibles.** Por ello, hemos incluido solamente algunas entidades privadas en el ámbito de aplicación subjetivo de la Proposición de Ley, previendo, sin embargo, la obligación de respetar el resto de derechos y obligaciones previstos por parte de los sujetos no incluidos en dicho ámbito de aplicación.

- ¿En qué sectores concretos debería garantizarse especialmente el cumplimiento por parte de las empresas de disponer de canales de denuncia internos?

Concretamente, en lo relacionado con esta pregunta, nuestra Proposición de Ley prevé lo siguiente:

Artículo 2.- Ámbito subjetivo de aplicación.

1. Las siguientes administraciones y entidades legales deben establecer canales de alerta anónimos y seguros, internos y externos, cumpliendo con las obligaciones establecidas en el Título III:

a) La Administración General del Estado, las Administraciones de las Comunidades Autónomas y de las Ciudades de Ceuta y Melilla.

b) Las entidades gestoras y los servicios comunes de la Seguridad Social así como las mutuas de accidentes de trabajo y enfermedades profesionales colaboradoras de la Seguridad Social.

c) Entidades de derecho público con personalidad jurídica propia de ámbito nacional y autonómico, los organismos autónomos, las Agencias Estatales y las entidades de Derecho Público que, con independencia funcional o con una especial autonomía reconocida por la Ley, tengan atribuidas funciones de regulación o supervisión de carácter externo sobre un determinado sector o actividad, incluyendo Autoridades Independientes.

d) El Defensor del Pueblo e instituciones autonómicas análogas.

e) El Consejo General del Poder Judicial y la Fiscalía General del Estado.

2. Las siguientes entidades deben establecer canales de alerta internos que cumplan con las obligaciones establecidas en el Título III:

a) Los partidos políticos, las organizaciones sindicales y las organizaciones empresariales.

b) Las sociedades mercantiles en cuyo capital social la participación, directa o indirecta, de las entidades previstas en este artículo sea superior al 50 por 100; las fundaciones y las asociaciones constituidas por las administraciones, organismos y entidades previstas en este artículo.

c) Administraciones del Estado, Autonómicas, Provinciales y Municipios con más de 10,000 residentes no incluidas en el apartado anterior, y en todo caso, la Casa de su Majestad el Rey, el Congreso de los Diputados, el Senado, el Tribunal Constitucional, así como el Banco de España, el Consejo de Estado, el Tribunal de Cuentas, el Consejo Económico y Social y las instituciones autonómicas análogas.

d) Entidades privadas con más de 50 trabajadores o de cualquier envergadura cuando operen en materia de servicios financieros u otras materias con riesgo de blanqueo de capitales.

e) Universidades.

3. Las Administraciones Públicas y las entidades jurídicas no incluidas en secciones anteriores, tanto en el sector público como privado, deben cumplir y respetar los derechos y obligaciones establecidos en la presente Ley para proteger alertadores y facilitadores.

4. Cualquier otra administración o entidad, pública o privada, incluyendo, pero sin limitarse a, los medios de comunicación, organizaciones no gubernamentales, organizaciones sindicales, miembros del poder legislativo, organizaciones y asociaciones profesionales, podrán establecer canales externos de alerta

- ¿Debería España exonerar a las entidades públicas de menos de 50 trabajadores de la obligación de establecer canales y/o mecanismos de denuncia internos?

Concretamente, en lo relacionado con esta pregunta, nuestra Proposición de Ley prevé lo siguiente:

Artículo 2.- Ámbito subjetivo de aplicación.

(...) 2. Las siguientes entidades deben establecer canales de alerta internos que cumplan con las obligaciones establecidas en el Título III:

(...) b) Las sociedades mercantiles en cuyo capital social la participación, directa o indirecta, de las entidades previstas en este artículo sea superior al 50 por 100; las fundaciones y las asociaciones constituidas por las administraciones, organismos y entidades previstas en este artículo.

(...) d) Entidades privadas con más de 50 trabajadores o de cualquier envergadura cuando operen en materia de servicios financieros u otras materias con riesgo de blanqueo de capitales.

(...) 3. Las Administraciones Públicas y las entidades jurídicas no incluidas en secciones anteriores, tanto en el sector público como privado, deben cumplir y respetar los derechos y obligaciones establecidos en la presente Ley para proteger alertadores y facilitadores.

4. Cualquier otra administración o entidad, pública o privada, incluyendo, pero sin limitarse a, los medios de comunicación, organizaciones no gubernamentales, organizaciones sindicales, miembros del poder

legislativo, organizaciones y asociaciones profesionales, podrán establecer canales externos de alerta.

Artículo 19.- Sistemas internos.

*(...) 2. Las entidades privadas con más de 50 trabajadores y menos de 249 podrán compartir recursos para la recepción e investigación de las alertas, sin perjuicio del cumplimiento de las obligaciones de confidencialidad, información del procedimiento a la y al alertador y abordar el incumplimiento detectado. **Los canales de recepción de alertas podrán ser compartidos entre municipios o por uniones de municipios siempre que se garantice que la información recibida y dirigida sólo a uno de ellos no es accesible por los otros.***

En un ejercicio de ponderación de las capacidades de las entidades consideradas pequeñas con la protección del interés general, creemos que **no sería proporcional obligar al establecimiento de estos canales, con todas las obligaciones y responsabilidades derivadas de ello, a entidades demasiado pequeñas cuando existan multiplicidad de canales externos accesibles.** Por ello, hemos incluido solamente algunas entidades privadas en el ámbito de aplicación subjetivo de la Proposición de Ley, previendo, sin embargo, la obligación de respetar el resto de derechos y obligaciones previstos por parte de los sujetos no incluidos en dicho ámbito de aplicación.

- ¿Debe permitirse que los canales de denuncia puedan ser gestionados tanto internamente por parte de una persona o departamento designado al efecto como externamente por parte de un tercero, sin perjuicio de que la responsabilidad de la llevanza del canal sea del órgano interno de la compañía o entidad?

Concretamente, en lo relacionado con esta pregunta, nuestra Proposición de Ley prevé lo siguiente:

Artículo 17.- Procedimiento de alerta

El procedimiento de alerta y de seguimiento de las alertas debe incluir y garantizar el cumplimiento de los siguientes aspectos: (...)

f) En su caso, la designación de uno, varios miembros del personal, un departamento o un tercero, que en todo caso deberá ser imparcial, como encargado de la recepción de las alertas, denominado administrador del canal.

I) En los canales de recepción de alertas que se operen por terceras entidades autorizadas a recibir alertas por parte de entidades públicas y privadas, deberán respetarse los principios de independencia, confidencialidad, protección de datos personales y secreto, además de los requisitos informativos mencionados en el artículo 16.

II) La o el administrador del canal se encargará de hacer un seguimiento diligente de la alerta, mantener la comunicación con la y el alertador, y en caso de ser preciso, solicitar información

adicional y mantener a la y al alertador informado del procedimiento seguido tras su alerta.

Con el consentimiento de la y el alertador, las y los administradores del canal serán responsables de remitir la información constitutiva de alerta a las instituciones competentes para que sea objeto de investigación.

III) Como prerrequisito, la o el administrador o administradores del canal deberán recibir formación profesional específica para gestionar canales de alerta.

IV) Todas las actividades del personal para cumplir con las responsabilidades que conllevan los canales de alerta estarán protegidas bajo esta Ley.

g) Las y los administradores de los canales de recepción de alertas deberán asegurarse que en caso de recibir una alerta a través de otros canales o por miembros del personal distintos a los encargados de su recepción, estos remitirán la alerta a los encargados preservando la confidencialidad de la información y sin modificar su contenido.

Artículo 19.- Sistemas internos.

(...) 2. Las entidades privadas con más de 50 trabajadores y menos de 249 podrán compartir recursos para la recepción e investigación de las alertas, sin perjuicio del cumplimiento de las obligaciones de confidencialidad, información del procedimiento a la y al alertador y abordar el incumplimiento detectado. Los canales de recepción de alertas podrán ser compartidos entre municipios o por uniones de municipios siempre que se garantice que la información recibida y dirigida sólo a uno de ellos no es accesible por los otros.

Así, se contempla tanto la posibilidad de gestionar internamente los canales de alerta, como que sea un proveedor externo quien lo haga, e incluso pudiendo compartir recursos cuando sea necesario, siempre cumpliendo los requisitos previstos legislativamente.

4. En relación con la obligación de establecer canales de denuncia externa en el artículo 11 de la Directiva:

- ¿Debe establecerse el archivo del procedimiento en caso de una infracción manifiestamente menor?

Toda alerta recibida debe ser objeto de análisis mediante el procedimiento correspondiente establecido por ley, no debiendo la ley establecer cuando una alerta debe o no archivers. En todo caso corresponderá dicha decisión al administrador del canal de alerta tras el análisis de la información proporcionada por la o el alertador y sucesivamente a las instancias siguientes a las que les corresponda investigar. En todo caso deberán preverse garantías

como la información y la justificación de la decisión a la o al alertador sobre el archivo, para que dicha decisión pueda ser recurrida y/o revisada.

Concretamente, en lo relacionado con esta pregunta, nuestra Proposición de Ley prevé lo siguiente:

Artículo 17.- Procedimiento de alerta

El procedimiento de alerta y de seguimiento de las alertas debe incluir y garantizar el cumplimiento de los siguientes aspectos: (...)

e) El acuse de recibo de la alerta, que deberá remitirse en un plazo máximo de 7 días desde su recepción si la alerta incluía los datos de contacto del alertador o facilitador.

l) Tras el análisis de la información proporcionada por la y el alertador y/o facilitador, mediante declaración-adjunta al acuse de recibo, la entidad deberá comunicar a la y al alertador y/o facilitador:

- Si considera que hay suficiente información para una mayor investigación;

- O que la misma no incluye información relevante o indicios consistentes sobre la infracción por lo que se considera la alerta cerrada. La y el alertador tendrá derecho a responder dicha determinación preliminar.

En el caso que la y el alertador o facilitador no esté de acuerdo con la decisión de la o el administrador del canal, podrá recurrir ante la Autoridad Independiente de Protección de las y los Alertadores y Facilitadores o ante la Jurisdicción competente.

ll) En caso de que una entidad no sea capaz de analizar y valorar la información recibida a efectos de emitir la declaración constitutiva anterior, por la voluminosidad de la información proporcionada, la entidad puede pedir el consentimiento del alertador y/o facilitador para trasladar la alerta a la Autoridad Independiente de Protección de los Alertadores y Facilitadores para que la misma proceda a realizar su seguimiento.

No podrán trasladar la información presuntamente constitutiva de alerta a la Autoridad, los Juzgados, Tribunales, Ministerio Fiscal y Fuerzas y Cuerpos de seguridad del Estado, quienes deberán en todo caso investigar la información constitutiva de alerta.

- ¿Debe disponerse que exista la posibilidad de archivar el procedimiento por lo que respecta a denuncias reiteradas que no contengan información nueva y significativa sobre infracciones en comparación con una denuncia anterior respecto de la cual han concluido los correspondientes procedimientos, a menos que se den nuevas circunstancias de hecho o de Derecho que justifiquen un seguimiento distinto?

Ídem pregunta anterior.

5. En relación con las autoridades competentes encargadas de recibir, dar respuesta y seguir las denuncias previstas en el artículo 11 de la Directiva:

- ¿Debe crearse una autoridad administrativa independiente encargada de recibir, dar respuesta y seguir las denuncias que se presenten por canales externos o deben encomendarse las funciones a una autoridad ya existente?

Como ya comentado, para mayor garantía, **la responsabilidad de implantar canales externos no debería limitarse a una sola autoridad y a las autoridades equivalentes a nivel autonómico, debiendo preverse su implantación en multitud de Administraciones para mayor accesibilidad** a estos canales, lo cual será positivo también para la cobertura del amplio objeto material que deberá cubrir la transposición.

Concretamente, en lo relacionado con esta pregunta, nuestra Proposición de Ley prevé lo siguiente:

Artículo 2.- Ámbito subjetivo de aplicación.

*1. Las siguientes administraciones y entidades legales deben establecer **canales de alerta anónimos y seguros, internos y externos**, cumpliendo con las obligaciones establecidas en el Título III:*

a) La Administración General del Estado, las Administraciones de las Comunidades Autónomas y de las Ciudades de Ceuta y Melilla.

b) Las entidades gestoras y los servicios comunes de la Seguridad Social así como las mutuas de accidentes de trabajo y enfermedades profesionales colaboradoras de la Seguridad Social.

c) Entidades de derecho público con personalidad jurídica propia de ámbito nacional y autonómico, los organismos autónomos, las Agencias Estatales y las entidades de Derecho Público que, con independencia funcional o con una especial autonomía reconocida por la Ley, tengan atribuidas funciones de regulación o supervisión de carácter externo sobre un determinado sector o actividad, incluyendo Autoridades Independientes.

d) El Defensor del Pueblo e instituciones autonómicas análogas.

e) El Consejo General del Poder Judicial y la Fiscalía General del Estado.

(...) 3. Las Administraciones Públicas y las entidades jurídicas no incluidas en secciones anteriores, tanto en el sector público como privado, deben cumplir y respetar los derechos y obligaciones establecidos en la presente Ley para proteger alertadores y facilitadores.

4. Cualquier otra administración o entidad, pública o privada, incluyendo, pero sin limitarse a, los medios de comunicación, organizaciones no gubernamentales, organizaciones sindicales, miembros del poder legislativo, organizaciones y asociaciones profesionales, podrán establecer canales externos de alerta.

Sobre Autoridad Independiente: Realmente **idealmente esta función debería ser encomendada a un juzgado específico**, como el de violencia de género.

La opción de una Autoridad Independiente es solo un repliegue para facilitar la aprobación de la Ley.

La autoridad, además de la función de recepción de alertas para decidir cuál es el mejor cauce social o institucional para que sea investigada, **deberá sobre todo encargarse de la protección de las y los alertadores** y no al revés. No se trata de crear una o varias "Stasi" que investiguen sin mandato judicial, sino de organismos que se encarguen de proteger las personas que alertan. Confundir estas dos funciones - aunque pueden verse unificadas en ciertos casos, como en el caso de la fiscalía - llevaría a un grave retorcimiento de la intención de la Directiva.

Así mismo, es necesario establecer mecanismos de coordinación, colaboración y cooperación entre la Autoridad y las agencias o entidades ya existentes o que se puedan crear a nivel autonómico o municipal, además de otros organismos y entidades que desarrollan funciones de naturaleza análoga o sobre la materia en el ámbito nacional, europeo o Internacional.

Dicho esto, de establecerse una Autoridad, inspiradas en el funcionamiento de Antifrau Valencia, estas deberían ser sus características para que no se transforme en un peligroso espacio de tráfico de información como sucedió a la Oficina Antifrau de Catalunya cuando fue dirigida por De Alfonso (<https://blogs.publico.es/el-blog-de-xnet/fernandez-diaz-daniel-alfonso-lucha-contra-corrupcion/>):

Artículo 23.- Fines y funciones

Son fines y funciones de la Autoridad:

- a) Actuará como canal externo anónimo y seguro, conforme al artículo 14.3, de recepción de alertas con información sobre infracciones.*
- b) Tal y como previsto en el artículo 17, emitir el acuse de recibo de las alertas recibidas a través del canal externo previsto en el apartado anterior y de aquellas que le sean transmitidas por administradores de canales internos o externos de recepción de alertas.*
- c) La Autoridad debe derivar de oficio las informaciones constitutivas de alerta sobre las que han informado a las instituciones, autoridades y entidades que sean competentes para llevar a cabo una investigación sobre las mismas, y en su caso, tramitarlas e iniciar los procedimientos administrativos o judiciales correspondientes sobre la información objeto de alerta.***
- d) Representar legalmente a la y al alertador y/o facilitador en todo procedimiento judicial y/o administrativo derivado de la alerta con el objetivo de no revelar su identidad y conservar la confidencialidad de su identidad.*
- e) Proporcionar asistencia jurídica gratuita, en coordinación con los Colegios Profesionales, a las y los alertadores y facilitadores. Esta asistencia jurídica comprenderá el asesoramiento sobre todos los aspectos relacionados con su alerta, así como también la representación y defensa jurídicas en todo procedimiento en que la y el alertador y/o facilitador sea parte, ya sea por querer iniciado o por ser parte demandada o denunciada en algún procedimiento, directamente vinculado con la alerta o causa de las represalias emprendidas con la intención de*

menoscabar su integridad física, moral, honor u opinión pública sobre la o el alertador o facilitador.

La Asistencia Jurídica Gratuita por parte de los Colegios de Abogados y Procuradores se prestará de acuerdo con el artículo 9 de la presente Ley y por las normas que sean aplicables y será solicitada por la Autoridad en representación de la y el alertador y/o facilitador.

Sin perjuicio de este servicio, la Autoridad deberá disponer de un servicio de asistencia jurídica permanente y eficaz para asesorar y aconsejar debidamente a las y los alertadores o facilitadores, o personas que estén considerando alertar, como mínimo en relación a la información contenida en el artículo 16, para que puedan tomar una decisión informada sobre cómo y cuándo hacerlo. Esta asistencia jurídica previa, amparada por los derechos de confidencialidad, anonimato y protección de datos personales, deberá poder ser solicitada y proporcionada mediante el canal previsto en el apartado a) del presente artículo, a las personas que lo soliciten de forma anónima.

f) En todo momento, la Autoridad velará para que las y los alertadores y/o facilitadores no sufran, durante su intervención, ni después de ella, ningún tipo de aislamiento, persecución o empeoramiento de las condiciones laborales o profesionales, ni ningún tipo de medida que implique cualquier forma de perjuicio o discriminación. Si la Autoridad es sabedora de que han sido objeto, directa o indirectamente, de actos de intimidación o de represalias por el hecho de alertar, podrá ejercer las acciones correctoras o de restablecimiento que considere, de las cuales dejará constancia en la memoria anual. En particular, a instancia de la o el alertador y/o facilitador, la Autoridad podrá instar al órgano o entidad competente a trasladarle a otro puesto, siempre que no implique perjuicio a su estatuto personal y carrera profesional y, excepcionalmente, podrá también instar al órgano competente a conceder permiso por un tiempo determinado con mantenimiento de la retribución.

A este fin, la Autoridad, así como los Juzgados o Tribunales y el Ministerio Fiscal, tendrán potestad para ordenar y solicitar de oficio, según corresponda, la aplicación de las medidas provisionales y cautelares de protección y de seguridad convenientes cuando pueda concurrir, a su juicio, la existencia de peligro grave para la persona, la libertad o los bienes de la o el alertador y/o facilitador, o el testigo, el cónyuge o la persona a quien se encuentre ligado por análoga relación de afectividad, o los ascendentes, descendientes o parientes del mismo hasta el segundo grado de consanguinidad o afinidad.

El órgano competente, si lo cree conveniente, podrá acordar y mantener estas medidas más allá de la resolución de los procedimientos judiciales y/o administrativos consecuencia de la alerta. La protección podrá mantenerse, mediante una resolución de la Autoridad, incluso más allá de la culminación de los procesos en los que la misma intervenga.

g) La colaboración con las y los administradores de canales internos y externos de recepción de alertas para la protección efectiva de alertadores y/o facilitadores que hayan utilizado sus canales.

h) Colaborar con las y los administradores de canales internos y externos de recepción de alertas para asegurar la efectividad de los mismos y la protección de las y los alertadores y facilitadores, con el establecimiento

de criterios previos, claros y estables de control de irregularidades e infracciones en el seno de las organizaciones e instituciones. Para asegurarse del cumplimiento de los mismos, la Autoridad podrá formular requerimientos dirigidos a las y los administradores de canales de recepción de alertas para que adapten o modifiquen sus protocolos o procedimientos de actuación.

i) Colaborar en la revisión periódica, y posterior adaptación, de los procedimientos de alerta establecidos por las y los administradores de canales de recepción de alertas que debe llevarse a cabo como mínimo una vez cada tres años. En este sentido, la Autoridad promoverá espacios y canales para con la sociedad civil donde se recogerán sus aportaciones para la mejora de los procedimientos.

En todo caso, la Autoridad deberá velar por la eficacia, integridad y eficiencia de estos procedimientos desde el punto de vista de protección de las y los alertadores y facilitadores e investigar y sancionar las posibles denuncias de ineficacia o abusos por parte de administradores de canales de recepción de alertas o terceros.

j) Supervisar y colaborar con las y los administradores de canales internos y externos de recepción de alertas para la formación del personal responsable de los mismos sobre: el contenido de la Ley de Protección Integral de las y los Alertadores y las medidas técnicas, organizativas y jurídicas a utilizar para garantizar el anonimato de las y los alertadores y facilitadores y su protección. Además, la Autoridad podrá elaborar guías formativas y de asesoramiento especializado en materia de protección de alertadores y facilitadores que recojan estos aspectos.

k) Contribuir a la creación de una cultura social de transparencia institucional, rechazo del fraude, la corrupción y el encubrimiento de las infracciones cometidas por los actores económicos y sociales, tanto públicos como privados.

l) Colaborar y elaborar propuestas de actuación con organismos que tengan funciones semejantes o de naturaleza análoga en el Estado, Comunidades Autónomas, en la Unión Europea o en el ámbito internacional.

m) Informar preceptivamente los proyectos normativos que desarrollen esta Ley u otros proyectos normativos que estén relacionados con su objeto.

n) Ejercer la potestad sancionadora en relación con las infracciones y sanciones establecidas en la presente Ley.

o) Todas las demás atribuciones que legalmente le sean atribuidas.

6. En relación con el artículo 23 de la Directiva, ¿qué tipo de sanciones aplicables considera que se pueden aplicar como efectivas, proporcionadas y disuasorias?

Concretamente, en lo relacionado con esta pregunta, nuestra Proposición de Ley prevé lo siguiente:

Artículo 37.- Infracciones.

1. Se consideran infracciones contra el régimen de protección de los derechos de las y los alertadores y facilitadores las acciones u omisiones que contravengan lo dispuesto en la presente Ley, a modo de ejemplo, y sin ánimo exhaustivo, aquellas que supongan:

- a) obstaculizar o el intento de obstaculizar alertas;
- b) acometer medidas de represalia o persecución contra las personas objeto de protección por la presente Ley
- c) acometer actos vejatorios contra las personas objeto de protección por la presente Ley
- d) vulnerar el deber de confidencialidad o anonimato sobre la identidad de las personas objeto de protección por la presente Ley y sobre la información objeto de alerta.

2. Las infracciones tipificadas en esta Ley se clasifican en muy graves, graves y leves:

a) Se consideran muy graves las siguientes actuaciones:

a.I) quebrantar las garantías de anonimato, confidencialidad, secreto y seguridad que esta Ley prescribe, así como de aquellas con que se hayan hecho públicos los canales de recepción de alertas;

a.II) revelar la identidad de la o el alertador cuando éste haya optado por el anonimato, incluyendo la identificación de la o el alertador anónimo, o la infracción de la regla de confidencialidad en su caso;

a.III) las acciones u omisiones tendentes a revelar la identidad de la o el alertador cuando éste haya optado por el anonimato o la confidencialidad aunque no se llegue a producir la efectiva revelación de la identidad de la o el alertador;

a.IV) la imposición de sanciones o la adopción de medidas arbitrarias, perjudiciales, persecutorias o de represalia por causa de la revelación de la alerta cuando hayan colocado en una situación de perjuicio personal a la y al alertador o facilitador que las haya sufrido, de forma directa o indirecta, o a su familia, compañeros o a los bienes y entidades propias o con las que estén conectados;

a.V) no haber tomado las precauciones indicadas en el artículo 4.9 en el caso de información catalogada como de seguridad nacional, secretos oficiales o militares, o información clasificada;

a.VI) publicitar un canal como anónimo y seguro sin que el mismo cumpla con las condiciones del artículo 14.3 o no informar que se trata de un canal que no es anónimo y seguro;

a.VII) la comunicación o publicación, por parte de una o un alertador o facilitador, de informaciones constitutivas de alerta que se hayan demostrado falsas, cuando la resolución que ponga término a la averiguación de los hechos generados por la alerta concluya que la información contenida en la alerta era falsa y declare expresamente que la o el alertador o facilitador conocían su falsedad en el momento de comunicarla o publicarla;

a.VIII) el incumplimiento de las obligaciones de secreto y confidencialidad de la información constitutiva de alerta y del resto de aspectos que el procedimiento de alerta establecido por la entidad debe garantizar conforme al artículo 17;

- a.IX) la suspensión o limitación de los derechos previstos por la presente Ley mediante cualquier tipo de acuerdo, convenio colectivo, política o contrato;*
- a.X) no disponer de un canal de recepción de alertas interno o externo cuando sea obligatorio de acuerdo con la presente Ley o normativa de desarrollo;*
- a.XI) el incumplimiento injustificado o contravención del deber de colaboración con la Autoridad Independiente de Protección de las y los Alertadores y Facilitadores, por ejemplo, no respondiendo ni realizando un seguimiento de los requerimientos de información y cumplimiento emitidos por la Autoridad Independiente de Protección de las y los Alertadores y Facilitadores.*
- a.XII) represalias o afectación al normal funcionamiento de los servicios de asesoramiento gratuito de alertadores y facilitadores ofrecidos por los Colegios de Abogados, la Autoridad Independiente o las organizaciones de la sociedad civil;*
- a.XIII) represalias o afectaciones contra cualquier persona que actúe en nombre de la Autoridad en el desempeño de sus funciones;*
- b) Se consideran graves las siguientes actuaciones:*
- b.I) la omisión de la información necesaria sobre la utilización de un canal de comunicación y recepción de alertas y la omisión, en todo o en parte, de la información prevista en el artículo 16;*
- b.II) la omisión del derecho a la información y acceso al procedimiento de los artículos 8, 19 y 20 de la presente Ley sin motivación sobre la puesta en peligro de la investigación;*
- b.III) la amenaza de inicio de expediente sancionador o de imposición de sanción disciplinaria a la y al alertador o facilitador, así como el inicio efectivo de los trámites para su imposición, cuando la misma no se haya llegado a imponer, siempre que esté relacionada con la comunicación de la información constitutiva de alerta;*
- b.IV) la imposición de sanciones o la adopción de medidas perjudiciales por causa de la revelación de la alerta cuando hayan provocado una situación de perjuicio personal y económico de carácter temporal a la y al alertador o facilitador que las haya sufrido, de manera que pueda ser dejada sin efecto y compensada razonablemente, siempre que el importe de dicha compensación se estime superior a DOS MIL EUROS (2.000,00 €);*
- b.V) el incumplimiento de las condiciones de custodia y almacenamiento de las alertas establecidas en el artículo 21;*
- b.VI) la exigencia de dirigirse en primer lugar a canales internos de alerta para poder utilizar canales externos o de justificar la elección del canal;*
- b.VII) no remitir a la autoridad que disponga de las competencias necesarias la alerta a la que la o el administrador del canal de recepción de alertas no pueda dar seguimiento por no disponer de las competencias necesarias;*
- b.VIII) la omisión del deber de revisión de los procedimientos y protocolos de alerta;*
- b.IX) la ineficacia manifiesta de los canales internos o externos de alerta proporcionados por las y los administradores.*
- c) Se consideran leves las siguientes actuaciones:*

- c.I) las tipificadas en los apartados b.I) y b.III) cuando por su escasa entidad y trascendencia no merezcan la consideración de graves;
- c.II) todas las demás actuaciones que contravengan lo dispuesto en esta Ley cuando concurran las circunstancias del párrafo b) anterior y el daño producido no se estime superior a los CINCO MIL EUROS (5.000,00 €).
- d) Cualquier otra actuación que atente contra la consecución de los objetivos de la presente Ley será sancionada con arreglo al criterio de proporcionalidad previsto en el artículo 39.

Artículo 38.- Sanciones.

1. Las infracciones muy graves se sancionarán con multa de 100.001 a 300.000 euros; las graves, con multa de 10.001 a 100.000 euros, y las leves, con multa de hasta 10.000,00 euros.

2. Asimismo las infracciones muy graves se sancionarán con **inhabilitación** hasta tres años; las graves, con inhabilitación hasta un año.

3. Cuando la infracción fuere cometida por funcionario público o personal al servicio de la administración pública, y la misma tuviere relación directa con sus atribuciones, le será impuesta la sanción de inhabilitación absoluta o especial de hasta tres meses si se trata de falta leve, de hasta un año si se trata de falta grave y de hasta tres años o separación del puesto si la falta cometida fuere de carácter muy grave.

4. En ningún caso podrá suspenderse o limitarse la aplicación de las sanciones previstas por la presente Ley por la aplicación de ningún acuerdo, convenio colectivo, política, contrato o acuerdo de arbitraje.

Artículo 39.- Proporcionalidad en la imposición de sanciones.

La graduación de la sanción considerará especialmente los siguientes criterios:

a) El grado de culpabilidad o la existencia de intencionalidad.

b) La continuidad o persistencia en la conducta infractora.

c) La naturaleza de los perjuicios causados.

d) La reincidencia, por comisión en el término de tres años de más de una infracción de la misma naturaleza cuando así haya sido declarado por resolución firme. Además la persistencia de la conducta infractora por acumulación transforma las infracciones de leves a graves y de graves a muy graves.

7. Entre las medidas de protección del denunciante, ¿deben incluirse premios o recompensas?

Si bien en otros países, como Estados Unidos o Alemania, tienen la consideración de alertadores las personas que actúen como tales a cambio de una remuneración económica o contraprestación patrimonial, **en el contexto español, con un alto grado de corrupción, por recomendación de del sindicato de técnicos del Ministerio de Hacienda (GESTHA), se considera más oportuno omitir esta posibilidad para que el criterio de convicción**

razonable sobre la veracidad de la información constitutiva de alerta no pudiera verse enturbiado por este supuesto y en ningún caso se pudiera entrar en la valoración de las motivaciones prácticas o éticas de la y el alertador.

Los alertadores actúan en beneficio del interés general y de forma desinteresada. **Prever un premio o recompensa, como lo ha hecho el grupo parlamentario de VOX en su Proposición de Ley registrada en el Congreso, no parece la forma adecuada de motivar a quienes sean testigos de conductas ilícitas para alertar sobre las mismas, sino ofrecerles la adecuada protección** sin pérdida de salario y con las debidas indemnizaciones por la posible pérdida de capacidad adquisitiva debida a su acto y otros daños y perjuicios derivados de la alerta.

Consideramos un problema recurrente querer vincular la efectividad de las pruebas obtenidas para atacar un ilícito a cuestiones morales. Consideramos que el objetivo de esta Directiva debe ser el de facilitar el descubrimiento de actos graves contra el interés general. A la luz de este objetivo es irrelevante si la persona que los destapa lo hace con buena o mala intención siempre y cuando correspondan a la verdad. El juicio moral sobre su conducta no debería ser objeto de la Directiva, aunque sí su eventual implicación en hechos delictivos. Por esto queremos subrayar la importancia de no implicar la intención sino únicamente la "*reasonable believe*" o sospecha razonable.

8. Finalmente, ¿qué otras cuestiones considera que se deberían contemplar al margen de la transposición de la Directiva?

Las cuestiones aquí abajo planteadas son cruciales y no deben ser consideradas de menor importancia solo por estar en el apartado "otras cuestiones".

8.1. PROBLEMÁTICA RELACIONADA CON EL USO DE LAS PALABRAS "DENUNCIANTE" Y "DENÚNCIA"

Utilizar la palabra "denunciante" para indicar los "whistleblowers", alertadores es un gravísimo error.

Nos sorprende que no se utilice el término "alertador" y "alerta" en el texto de la presente consulta ni una sola vez. Parece que no se haya considerado por el Grupo de Trabajo de la Comisión General de Codificación para la transposición de la Directiva (https://ficheros.mjusticia.gob.es/Orden_constitucion_2_junio_2020.pdf). **Es francamente sorprendente tenido en cuenta que el propio Ministro de Justicia, Juan Carlos Campo, en una de sus primerísimas intervenciones públicas hizo manifestaciones explícitamente en acuerdo con nuestra petición ante la Comisión Europea y a la Delegación Permanente de España en Europa de que la traducción de la Directiva Europea para defender los alertadores (whistleblowers) no desactivase su función en la transposición al**

ordenamiento jurídico español, manifestando la necesidad de no utilizar el término “Denunciante” para hablar de “Alertadores” en la transposición de la Directiva europea (<https://xnet-x.net/peticion-rectificacion-traduccion-alertadores-recogida-ministro-justicia/>) por los siguientes motivos:

Los conceptos de denuncia y denunciante ya disponen de definiciones en el ordenamiento jurídico español, en los artículos 259 a 269 de la Ley de Enjuiciamiento Criminal, e impone obligaciones que entran en conflicto con lo previsto en la Directiva:

- **Obligatoriedad de “denunciar”**, cuando en la mayoría de los casos, como advierte la Directiva con la implantación de canales internos de alerta, no es lo más conveniente para resolver el problema planteado.
- Tanto las normas procesales penales como administrativas imponen denunciar de forma obligatoria **ante autoridades, órganos o instituciones específicos. Este hecho excluye la posibilidad de utilizar canales internos existentes en las empresas u otros canales, como el aviso a superiores u otros, y limita la libertad establecida en la Directiva para que los alertadores elijan el canal o canales que consideren adecuados** según sus circunstancias individuales.
- **Tanto en el ámbito administrativo como penal se exige que la persona se identifique, además de firmar la denuncia en el ámbito penal.** Este hecho contradice el anonimato permitido por la Directiva con el objetivo de proteger a los alertadores. En el ordenamiento jurídico español ya se admiten las alertas anónimas, concretamente en las materias de protección de datos personales y prevención de blanqueo de capitales, pero no se han establecido mecanismos jurídicos concretos para garantizar esta posibilidad. Aunque ya hay instituciones públicas que de facto ya reciben información anónima, la transposición de la Directiva debe servir para garantizar la legalidad de esta posibilidad y el uso del término “denunciante” compromete esta oportunidad.
- La definición de denunciante prevista en el ordenamiento actual limita el ámbito de aplicación material previsto por la Directiva. **El ámbito material de aplicación de la Directiva no se limita a delitos públicos o semipúblicos, sino que quiere ir más allá, permitiendo alertar sobre irregularidades, malas prácticas, abusos, u otros actos u omisiones que no son formalmente ilegales pero que consiguen frustrar el objetivo o propósito de la legislación y que afecten al interés público.** Así, la remisión a la definición jurídica de denunciante limitaría la aplicación de la Directiva en el ámbito nacional, contradiciendo su intención principal de proteger a los alertadores sea cual sea la infracción de la que alerten.
- **Ya se han tomado algunas precauciones en el ámbito nacional para evitar los efectos del uso del término “denunciante”.** En las leyes de protección de datos y prevención de blanqueo de capitales puede observarse como se excluye la palabra “denuncia” o “denunciante” y se opta por otros términos como “mecanismos de comunicación” o “información” para permitir que estas comunicaciones se realicen de forma anónima. También encontramos jurisprudencia española dónde se menciona el término de “whistleblower” para remarcar su ámbito de aplicación más amplio para la denuncia de actuaciones irregulares,

fraudulentas, abusivas o de mala gestión, y así diferenciar el alertador del “denunciante”. Finalmente, debe hacerse constar que el término “alertador” ya se ha utilizado ordenamiento jurídico español con anterioridad, publicándose en el BOE de 30 de noviembre de 2018.

El término “denunciante” podría resultar en la ineffectividad de la legislación, teniendo en cuenta que se trata de una palabra que desde una perspectiva social y cultural tiene connotaciones peyorativas, negativas y estigmatizantes.

Finalmente, utilizar el término "denunciante" podría conllevar un agravio respecto a los demás Estados miembros porque en otras traducciones de la Directiva se utilizan términos amplios que mantienen la neutralidad jurídica necesaria para respetar las disposiciones de la Directiva y que no conllevan las implicaciones jurídicas ni las connotaciones negativas que encontramos en la traducción española.

- En la versión inglesa, se utilizan los términos “whistleblower” y “reporting person”. El término “report” no conlleva las consecuencias jurídicas que sí comporta el uso del término “denuncia”. Por ejemplo, cuando una persona reporta información, la misma no tiene por qué constituir un ilícito penal, pudiendo tratarse de infracciones administrativas y civiles, y la “reporting person” puede no revelar su identidad. Por lo tanto, el uso de estos términos respeta la letra y el espíritu de la Directiva que prevé estas posibilidades. Debe encontrarse y utilizarse un término con la misma neutralidad que “report” en inglés que deje abiertas estas posibilidades de informar sobre irregularidades sin necesidad de identificarse y que no se trate de ilícitos penales. No encontrar este término reduce automáticamente el ámbito de aplicación y protección de la ley, causando un grave perjuicio para su correcta transposición.
- Utilizar el término “denunciante” equivaldría a que en la versión francesa en lugar de utilizar los términos “signalement” y “lanceur d’alerte” se hubiese utilizado el término “plainte”. En el mismo sentido, equivaldría que en la versión italiana se hubiese utilizado el término “denuncia” en lugar de utilizar los términos “persona segnalante” o “informatore”. Esto habría modificado gravemente el sentido y objetivo de la ley nacional, como pasa en el caso de la versión española.

Así, utilizar los términos “alertador”, “alerta” y “canales de alerta” mantendría la esencia de la normativa para favorecer la protección de los alertadores en el ámbito nacional, sin reducir el nivel de protección buscado por la directiva incluso con anterioridad a la transposición nacional.

La consulta pública se centra sobre el concepto de “denunciante”, ignorando el concepto de "alertador" recomendado por organizaciones civiles y reconocidos expertos para la traducción de "whistleblower", lo cual puede derivar en una protección restrictiva en la transposición de la Directiva, como explicamos aquí: <https://xnet-x.net/xnet-denuncia-traduccin-directiva-europea-para-defender-alertadores-whistleblowers/>

8.2. EXENCIÓN DE RESPONSABILIDAD E INVERSIÓN DE LA CARGA DE LA PRUEBA

Es de vital importancia garantizar que la revelación de información no conlleve la comisión de infracción por parte de las personas alertadoras y/o facilitadoras.

El alertador aporta una *notitia criminis* para que se investigue, la responsabilidad de averiguar si los indicios revelan la comisión un delito, irregularidad o abuso debe recaer en quien investiga. Además, **es contraproducente que una Ley que debería servir para compensar una asimetría de recursos y poder entre una persona y entidades poderosas, deje en mano de la primera la responsabilidad de demostrar que no ha cometido toda una serie de ilícitos antes de que se la proteja. Debe ser al revés.**

Concretamente, en lo relacionado con esta cuestión, nuestra Proposición de Ley prevé lo siguiente:

Artículo 4.- Informaciones que constituyen alerta.

(...) 2. No será un obstáculo para la comunicación y recepción de la información constitutiva de alerta el hecho que incluya:

a) Datos personales o datos especialmente protegidos, tal y como definidos en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, al amparo del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 General de Protección de Datos y de acuerdo con la sentencia del Tribunal Europeo de Derechos Humanos sobre el caso Hungarian Helsinki Committee respecto al FOI, en aras de garantizar el pleno respeto del derecho a la información.

En el caso de que la información se haga pública, esta excepción solo cubrirá la información personal directamente relacionada con las actuaciones ilícitas objeto de la alerta (como la identificación o nombre de la/s persona/s). Deberán omitirse los datos personales relacionados con el ámbito privado de las personas afectadas y que no aportan ningún valor informativo (como números de teléfono personal, dirección de correo electrónico personal, dirección del domicilio particular, ...). El cumplimiento de esta salvedad será responsabilidad de quien realice la publicación.

La excepción no se extenderá en ningún caso a la publicación de información relacionada con terceras personas a las que no les sean de ningún modo imputables tales actuaciones. Estas personas han de permanecer inidentificables. El cumplimiento de esta salvedad será responsabilidad de quien realice la publicación.

Cuando se cumpla con estas condiciones, la alerta no podrá considerarse difamación, calumnia, injuria o menoscabo contra el honor y la intimidad de la persona afectada.

b) Secretos, según la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.

c) Secretos empresariales, según la Ley 1/2019, de 20 de febrero, de Secretos Empresariales y la Directiva (UE) 2016/943 del Parlamento

Europeo y del Consejo, de 8 de junio de 2016, relativa a la protección de los conocimientos técnicos y la información empresarial no divulgados (secretos comerciales) contra su obtención, utilización y revelación ilícitas.

d) Revelaciones, según la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo y la Directiva 2005/60/CE del Parlamento Europeo y del Consejo, de 26 de octubre de 2005, relativa a la prevención de la utilización del sistema financiero para el blanqueo de capitales y para la financiación del terrorismo.

3. Tampoco será obstáculo para la comunicación, recepción o divulgación de la información que constituya una alerta que la misma se encuentre bajo la protección del Real Decreto Legislativo 1/1996, de 12 de Abril, por el que se aprueba el Texto Refundido de la Ley de Propiedad Intelectual.

4. No será obstáculo para la comunicación, recepción o divulgación de la información constitutiva de una alerta la protección garantizada por las normas profesionales, comerciales y empresariales aplicables cuando dicha información sea parte de la alerta.

5. Se considera información constitutiva de alerta cuyo acceso gozará de inmunidad, tanto la información a la que se ha tenido acceso directamente durante el desempeño de una actividad incluso si su comunicación constituye un incumplimiento de contrato u otras cláusulas sobre la propiedad de la información, como en los casos en que se acceda o se haga copia de información constitutiva de alerta en el ámbito civil, administrativo o laboral a la que normalmente no se tendría acceso, como, a modo de ejemplo y no de forma exhaustiva, el acceder a los correos electrónicos de un compañero de trabajo o a archivos de un departamento laboral al que normalmente no se tiene acceso.

El origen de la información no se tendrá en consideración para su calificación como información constitutiva de alerta.

6. La revelación de una alerta de acuerdo con las disposiciones de esta Ley no constituye un incumplimiento de las normas y cláusulas de confidencialidad, las relativas a secretos, a la propiedad intelectual e industrial o a la protección de datos personales, previstas en cualquier contrato administrativo, laboral, civil, mercantil o de cualquier otra naturaleza, y por lo tanto, la o el alertador no podrá ser considerado responsable de su incumplimiento en base a las reglas de responsabilidad civil, penal o disciplinaria que pudiesen resultar de aplicación.

7. Es nula de pleno derecho cualquier cláusula contractual cuyo propósito sea el de limitar o prohibir a alguien alertar o limitar el acceso al derecho de protección garantizado por la presente Ley.

8. En los procedimientos judiciales en que se juzgue el daño sufrido por la o el alertador y/o facilitador a causa de represalias que han sido consecuencia de la alerta por él realizada, se presumirá que el perjuicio se causó en represalia por la alerta. En tales casos, corresponderá a la persona que haya llevado a cabo la acción perjudicial probar que esta medida se fundó en motivos debidamente justificados y justos y que no estuvo relacionada de ninguna manera con la alerta.

9. En los casos en que la información constitutiva de alerta esté catalogada como de seguridad nacional, secretos oficiales o militares, o información clasificada, secreto profesional y de las comunicaciones entre

clientes y sus abogados, secreto profesional y de las comunicaciones entre los profesionales de la salud y sus pacientes, secreto de las deliberaciones judiciales la misma podrá ser objeto de comunicación y recepción, pero no podrá ser objeto de divulgación pública indiscriminada sino que deberán tomarse las precauciones necesarias para que pueda conocerse el ilícito, sin poner en peligro la seguridad nacional. La divulgación pública se considerará justificada en casos de amenazas urgentes o graves a la salud pública, a la seguridad y defensa del Estado, de las relaciones internacionales de Estado, o el medio ambiente.

Artículo 13.- De la responsabilidad de la y el alertador y facilitador.

1. La y el alertador y el facilitador deben únicamente tener una convicción razonable en la verosimilitud y fiabilidad de la información que comuniquen, que, como indicado en el artículo 4.1 debe ser información relevante e indiciaria. La responsabilidad de la comprobación de los hechos objeto de la alerta, de determinar si hay suficiente información para investigar las posibles infracciones y de la cualificación de los mismos como posibles delitos o acciones contra el interés general recae, en todo caso, sobre el organismo o institución a cargo de la investigación.

2. Cuando la resolución que ponga término a la averiguación de los hechos generados por la alerta concluya que no se trate de irregularidades, infracciones, malas prácticas o hechos constitutivos de ilícito penal, la y el alertador o facilitador mantendrá la protección reconocida por la presente Ley y no sufrirá perjuicio, sanción, o represalia alguna, a menos que se pruebe que la persona conocía la falsedad de la información en el momento de la alerta e informó deliberadamente sobre la misma.

3. Con la misma excepción señalada en el apartado anterior, la y el alertador y el facilitador no serán responsables por los daños y perjuicios que puedan derivarse de la comunicación o divulgación de la alerta o de las acciones realizadas para revelar la información, ni incurrirán en ningún otro tipo de responsabilidad, ya sea disciplinaria, civil o penal, que pueda derivar de tales circunstancias, incluidas expresamente las concernientes al posible menoscabo del derecho al honor, de los derechos de autor, de los secretos, secretos comerciales, prevención de blanqueo de capitales y de la protección de datos personales.

4. A la y al alertador y/o facilitador que hubiesen sido partícipes en los hechos objeto de la información constitutiva de alerta les será de aplicación la 7ª atenuante cualificada prevista por el artículo 21.7ª del Código Penal, para que la pena a la que podrían ser condenados sea la inferior en uno o dos grados.

8.3. USO INDEBIDO DE LA PROTECCIÓN DE DATOS (Y OTROS DERECHOS Y LIBERTADES)

Se están cometiendo abusos con una interpretación errónea de la legislación sobre protección de datos.

Este mal uso acarea graves perjuicios al derecho a la información, a la rendición de cuentas, la transparencia y a la labor de los periodistas, entre otros.

Como comentado, de lo que trata en general la protección de los alertadores es de corregir la asimetría entre los poderes fácticos y la gente de a pie.

No es baladí que cuando un alertadores saca a la luz unos abusos, la respuesta de quien los perpetra no suele ser discutir o solucionar el abuso en cuestión, sino atacar el alertador sobre temas inherentes a la ofensa íntima y arrollarlo con juicios de este tipo.

En nuestra larga experiencia, mientras hace unos años los poderosos respondían prácticamente siempre abriendo demandas sobre delitos contra el honor o delitos contra la propiedad intelectual o los secretos comerciales (de ahí la larga batalla durante la aprobación de la Directiva de Secretos Comerciales de 2016 – <http://blogs.publico.es/el-blog-de-xnet/secretos-comerciales/>) – es necesario también un mejor articulado sobre estos extremos – , ahora está de moda acusar de revelación de datos personales.

Naturalmente nosotros somos activos defensores de los derechos a la privacidad de las personas de a pie. Pero también somos activos defensores de la importancia de la transparencia de las instituciones públicas y grandes corporaciones de sus miembros, justamente para rectificar la asimetría de la que hablamos (<https://xnet-x.net/transparencia-y-privacidad/>), objetivo de la Directiva que nos ocupa.

Como indicado en el articulado del punto anterior, **la protección de datos no puede ni debe usarse como excusa para no denunciar ilegalidades** (se indica en el Reglamento Europeo de Protección de Datos arts. 85-86). Del mismo modo, en este ámbito no se puede usar el mismo baremo que se usa con un ciudadano corriente cuando se trata de servidores públicos o de directivos de empresas que repercuten sobre la gran mayoría de la población – a esos se limita el alcance de esta Directiva.

Como hemos dicho anteriormente, muchas veces los abusos no son tratados con efectividad si no se hacen públicos. Y no se pueden hacer públicos si no se indican las personas supuestamente responsables de los mismos.

Por esta razón, en aras de garantizar el pleno respeto de la libertad de expresión y de información que enuncia la Directiva, solo los datos personales relacionados con el ámbito privado y que no aportan ningún valor informativo – datos tales como números de teléfono, dirección de correo electrónico, dirección del domicilio, así bien como los de privados y personas no responsables del ilícito, deben permanecer ocultos en todo momento y prevalecer sobre la libertad de información.

En este sentido ya se ha expresado la sentencia del Tribunal Europeo de Derechos Humanos sobre el caso del Comité húngaro de Helsinki.

Se ha entonces de recalcar que la carga de la prueba debe favorecer el alertador y, como ya hemos dicho, su objetivo y razones no deben reducir la utilidad objetiva de sus revelaciones – no olvidemos que **el objetivo último de la Directiva no es moral sino el de eliminar los abusos de las instituciones.**

Los alertadores no son santos ni diablos, sus razones personales son...personales. **El aura romántica alrededor de los alertadores debe cesar, para que la práctica sacar a la luz abusos sea una normalidad en una sociedad democrática.** Esto debería ser el objetivo último de la Directiva.

8.4. PROTECCIÓN DE LAS Y LOS FACILITADORES E INTERMEDIARIOS

La protección garantizada por la Ley no sólo debe ser para las personas alertadoras conocedoras de informaciones sobre fraudes o actuaciones corruptas de las corporaciones públicas y privadas incluidas en el ámbito de esta norma, sino también para las y los facilitadores de las alertas: personas físicas o jurídicas tales como ONGs, plataformas ciudadanas, víctimas o medios de comunicación, entre otros, que suelen ser imprescindibles para que aflore la alerta dada por una o un alertador.

La superposición de facilitadores es una práctica común de los *whistleblowers* o alertadores cuando encuentran quien les garantice su anonimato y seguridad personal y familiar, que es el objetivo prioritario que persigue la Directiva y su transposición, siendo compatible el sistema de garantías de las y los alertadores también para la protección de las y los facilitadores en su caso, quienes también se ven expuestos a represalias.

No considerar que quienes destapan abusos de poderosos casi siempre necesitan la ayuda de alguien, es negar la realidad y legislar sin tenerlos en cuenta. Además, socavaría la importante función de la profesión periodística y la acción de ONGs y grupos ciudadanos activos en la defensa del bien común.

Concretamente, en lo relacionado con esta pregunta, nuestra Proposición de Ley prevé lo siguiente:

Artículo 3.- Definiciones y ámbito subjetivo de protección.

A los efectos de esta Ley se entiende por:

(...) b) Facilitador o facilitadora: cualquier persona física o jurídica que contribuye, facilita o ayuda a la o el alertador a revelar o hacer pública la información constitutiva de una alerta, incluyendo, pero sin limitarse a los siguientes: organizaciones de la sociedad civil, asociaciones y órganos profesionales, sindicatos, periodistas, organizaciones de periodistas y abogados.

Artículo 5.- Derechos que asisten a la o el alertador y facilitador.

Se garantiza el derecho de las y los alertadores y facilitadores a la seguridad, al anonimato y a la confidencialidad de su identidad, incluso frente a quienes reciban la alerta y quienes gestionen el procedimiento resultante de la misma, al acceso a la información del procedimiento, al asesoramiento jurídico y a la indemnidad. En ningún caso podrá suspenderse o limitarse la aplicación de los derechos y sanciones

previstos por la presente Ley por la aplicación de ningún acuerdo, convenio colectivo, política, contrato o acuerdo de arbitraje.

8.5. MEDIDAS DE PROTECCIÓN DE LAS PERSONAS ALERTADORAS Y FACILITADORAS Y SU ENTORNO

Es imprescindible prever mecanismos para que la protección de las personas alertadoras y/o facilitadoras se garantice y extienda a aquellas a las que esté relacionada por vínculos familiares o afectivos, así como las entidades jurídicas propiedad del alertador con las que tenga relación de propiedad, laboral, o de otro tipo, y que las represalias puedan ser sancionadas incluso cuando no hayan sido consumadas, incluso en caso de amenazas de represalias y de tentativas de represalia. El concepto de represalia debe ser un concepto amplio cuya interpretación no sea restrictiva.

Concretamente, en lo relacionado con esta cuestión, nuestra Proposición de Ley prevé lo siguiente:

Artículo 6.- Derecho a la seguridad y prohibición de las represalias.

1. Se prohíben las represalias, directas o indirectas y de cualquier tipo, incluyendo sin limitarse a discriminaciones, amenazas, recomendaciones e intentos de represalias, contra la persona, familia, compañeros, superiores, o los bienes y entidades propias o con las que estén conectados, si corresponde, las y los alertadores y/o facilitadores.

2. Las y los alertadores y facilitadores tienen derecho a recibir protección policial. Serán de aplicación todas las medidas cautelares de protección preventiva indicadas en la Ley Orgánica 19/1994, de 23 de diciembre, de protección a testigos y peritos en causas criminales por la autoridad (Título IV) y en el Estatuto de la Víctima, para detener y evitar las amenazas, peligros y represalias dirigidas a la o el alertador y/o facilitador su integridad física o sobre sus bienes.

3. Las mismas medidas se aplicarán, cuando fuere necesario, a sus cónyuges o personas ligadas por análoga relación de afectividad, así como a los familiares de ambos hasta el segundo grado de consanguinidad o afinidad, así como a otras contra quienes se tomen represalias por asistir o estar vinculado con la o el alertador y/o facilitador.

Artículo 23.- Fines y funciones

Son fines y funciones de la Autoridad: (...)

f) En todo momento, la Autoridad velará por que las y los alertadores y/o facilitadores no sufran, durante su intervención, ni después de ella, ningún tipo de aislamiento, persecución o empeoramiento de las condiciones laborales o profesionales, ni ningún tipo de medida que implique cualquier forma de perjuicio o discriminación. Si la Autoridad es sabedora de que han sido objeto, directa o indirectamente, de actos de intimidación o de represalias por el hecho de alertar, podrá ejercer las acciones correctoras o de restablecimiento que considere, de las cuales dejará constancia en la memoria anual. En particular, a instancia de la o el alertador y/o

facilitador, la Autoridad podrá instar al órgano o entidad competente a trasladarle a otro puesto, siempre que no implique perjuicio a su estatuto personal y carrera profesional y, excepcionalmente, podrá también instar al órgano competente a conceder permiso por un tiempo determinado con mantenimiento de la retribución.

A este fin, la Autoridad, así como los Juzgados o Tribunales y el Ministerio Fiscal, tendrán potestad para ordenar y solicitar de oficio, según corresponda, la aplicación de las medidas provisionales y cautelares de protección y de seguridad convenientes cuando pueda concurrir, a su juicio, la existencia de peligro grave para la persona, la libertad o los bienes de la o el alertador y/o facilitador, o el testigo, el cónyuge o la persona a quien se encuentre ligado por análoga relación de afectividad, o los ascendentes, descendientes o parientes del mismo hasta el segundo grado de consanguinidad o afinidad.

El órgano competente, si lo cree conveniente, podrá acordar y mantener estas medidas más allá de la resolución de los procedimientos judiciales y/o administrativos consecuencia de la alerta. La protección podrá mantenerse, mediante una resolución de la Autoridad, incluso más allá de la culminación de los procesos en los que la misma intervenga.

8.6. USO DE TÉRMINOS AMBIGUOS

Una interpretación sesgada de la Directiva y de la Ley no solo trasformaría su transposición al ordenamiento español en papel mojado, sino que podría conducir a una situación todavía peor para las personas que sacan a la luz pública corrupción y abusos (<https://blogs.publico.es/dominiopublico/33072/la-proteccion-de-las-y-los-alertadores-que-ayudan-a-destapar-abusos-y-corrupcion-no-puede-ser-interpretable-debe-ser-un-hecho-el-caso-de-roberto-macias/>), por ello es imprescindible que los términos utilizados en la redacción sean claros y no den lugar a ambigüedades.