LOS CANALES DE DENUNCIA Y LA PROTECCIÓN DEL INFORMANTE EN LAS ENTIDADES DEL SECTOR PRIVADO: A PROPÓSITO DE LA TRASPOSICIÓN DE LA DIRECTIVA (UE) 2019/1937, DE 23 DE OCTUBRE

José León Alapont[1]

Profesor Ayudante Doctor de Derecho Penal - Universidad de Valencia

Title: *Reporting channels and informant protection in private sector entities: regarding the transposition of Directive (EU) 2019/1937, of October 23*

Resumen: Los canales de denuncia en el ámbito privado cobraron una especial importancia a raíz de la inclusión en 2015 de los programas de cumplimiento como causa de exención/atenuación de la responsabilidad penal de las personas jurídicas. Ahora, años después, el legislador español está pendiente de la aprobación de una ley de protección del informante que viene a trasponer en buena medida la normativa europea existente al respecto. Al análisis de estas cuestiones dedicaremos el presento trabajo.

Palabras clave: canales de denuncia; *compliance*; personas jurídicas; denunciante; protección jurídica.

Abstract: *Reporting channels in the private sphere gained special importance as a result of the inclusion in 2015 of compliance programs as a cause of exemption/mitigation of the criminal liability of legal entities. Now, years later, the Spanish legislator is in the process of approving a whistleblower protection law that largely transposes the existing European*

[1] El presente artículo se enmarca en el Proyecto de Investigación «El Derecho penal frente a las crisis sanitarias» (GV/2021/103), concedido por la Conselleria de Innovación, Universidades, Ciencia y Sociedad Digital de la Generalitat Valenciana por el periodo 2021-2022. Siendo Investigador Principal del mismo.

regulations in this regard. To the analysis of these questions we will dedicate the present work.

Keywords: *complaint channels; compliance; legal persons; whistleblower; legal protection.*

Sumario: 1. Planteamiento. - 2. Los canales de denuncia en el marco del *compliance* penal. - 3. Aspectos prácticos. - 3.1. ¿Quién puede denunciar? - 3.2. ¿Qué se puede denunciar? - 3.3. ¿Qué consecuencias puede generar, en su caso, no denunciar estando «obligado» a ello? - 3.4. El eterno debate: ¿canal de denuncias anónimo o confidencial? - 4. Los diferentes escenarios que se le plantean al denunciante, al receptor directo de la comunicación y a la persona jurídica involucrada. - 5. La trasposición de la Directiva (UE) 2019/1937, de 23 de octubre: el Anteproyecto de Ley reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción. - 5.1. Sujetos obligados del sector privado. - 5.2. Materias objeto de denuncia. - 5.3. Sujetos que gozan de protección. - 5.4. Medidas de protección y de apoyo. - 5.4.1. Requisitos para la concesión de protección. - 5.4.2. Prohibición de represalias: listado. - 5.4.3. Exclusión de la responsabilidad en que se hubiere podido incurrir a raíz de la denuncia. - 5.4.4. Los denominados «programas de clemencia»: repercusión en el ámbito administrativo. - 5.4.5. Medidas de apoyo. - 5.5. Los «Sistemas internos de información»: disposiciones generales. - 5.5.1. Sujetos u órganos responsables de su implantación y gestión. - 5.5.2. Diseño de los sistemas internos de información. - 5.5.3. La externalización de la gestión del sistema. - 5.5.4. Tipos de canales internos de información. - 5.5.5. El procedimiento de gestión de las comunicaciones recibidas. - 5.6. Disposiciones comunes a los canales internos. - 5.7. Protección de datos. - 5.8. La Autoridad Independiente de Protección del Informante: aspectos principales. - 5.8.1. Funciones y ámbito competencial. - 5.8.2. Aspectos procedimentales. - 5.9. Revelación pública. - 5.10. Infracciones y sanciones. - 6. A modo de reflexión final. - 7. Bibliografía.

1. Planteamiento

La existencia de canales de denuncia a los cuales acudir para informar de hechos que posiblemente constituyan una «infracción» del ordenamiento jurídico (administrativo, penal, tributario, etc.) no son una novedad en nuestro país. Piénsese, por ejemplo, en la Agencia Tributaria, el Defensor del Pueblo, los Tribunales de Cuentas, Agencias Autonómicas Antifraude, el SEPBLAC, la CNMV, la CNMC, etc. En igual sentido, cabría advertir de la preocupación que desde instancias supranacionales se ha mostrado respecto de esta cuestión desde hace ya algún tiempo (cítese, a título de ejemplo, la ONU[2], la OCDE[3], o la propia Unión Europea[4]).

[2] Convención de las Naciones Unidas contra la corrupción, hecha en Nueva York el 31 de octubre de 2003. El art. 33, bajo la rúbrica «protección de los denunciantes» establece que: «cada Estado Parte considerará la posibilidad de incorporar en su ordenamiento jurídico interno medidas apropiadas para proporcionar protección contra todo trato injustificado a las personas que denuncien ante las autoridades competentes, de buena fe y con motivos razonables, cualesquiera hechos relacionados con delitos tipificados con arreglo a la presente Convención», contemplando en su artículo 8.4 el establecimiento de sistemas para facilitar que los funcionarios públicos denuncien todo acto de corrupción a las autoridades competentes, y en su artículo 13.2 la posibilidad de la denuncia anónima.

[3] A destacar el Informe «Committing to Effective Whistleblower Protection».

[4] Así, por ejemplo, la Directiva 2013/36/UE del Parlamento Europeo y del Consejo, de 26 de junio de 2013, relativa al acceso a la actividad de las entidades de crédito y a la su-

Sin embargo, estos mecanismos han cobrado un especial protagonismo a raíz de la inclusión de los *compliance programs* en el Código Penal[5].

Con todo, no debemos perder de vista que, en puridad, las únicas posibilidades de interponer una denuncia (como tal) son las que contempla nuestra LECrim. Y, por ello, aquí estamos ante otra suerte de «denuncias». Efectivamente, no pueden considerarse como tales, por lo que más correctamente cabría hablar de comunicaciones, de informaciones, de alertas, etc.

Como decíamos, aquellas personas jurídicas sujetas al ámbito de aplicación del art. 31 bis CP[6] estarán interesadas en incorporar esta herra-

---

pervisión prudencial de las entidades de crédito y las empresas de inversión, por la que se modifica la Directiva 2002/87/CE y se derogan las Directivas 2006/48/CE y 2006/49/CE (en relación con el Reglamento (UE) núm. 575/2013 del Parlamento Europeo y del Consejo, de 26 de junio de 2013, sobre los requisitos prudenciales de las entidades de crédito y las empresas de inversión, y por el que se modifica el Reglamento (UE) núm. 648/2012). El Reglamento (UE) núm. 376/2014 del Parlamento Europeo y del Consejo, de 3 de abril de 2014, relativo a la notificación de sucesos en la aviación civil, que modifica el Reglamento (UE) núm. 996/2010 del Parlamento Europeo y del Consejo, y por el que se derogan la Directiva 2003/42/CE del Parlamento Europeo y del Consejo y los Reglamentos (CE) núm. 1321/2007 y (CE) núm. 1330/2007 de la Comisión. La Directiva 2013/54/UE del Parlamento Europeo y del Consejo, de 20 de noviembre de 2013, sobre determinadas responsabilidades del Estado del pabellón en materia de cumplimiento y control de la aplicación del Convenio sobre el trabajo marítimo, de 2006. La Directiva 2009/16/CE del Parlamento Europeo y del Consejo, de 23 de abril de 2009, sobre el control de los buques por el Estado rector del puerto. O la Directiva 2013/30/UE del Parlamento Europeo y del Consejo, de 12 de junio de 2013, sobre la seguridad de las operaciones relativas al petróleo y al gas mar adentro, y que modifica la Directiva 2004/35/CE).

[5] A este respecto, Bachmaier Winter señala que el régimen de eximentes/atenuantes previsto en el art. 31 bis CP «ha actuado de facto como un catalizador para su implantación». *Vid*. Bachmaier Winter, L.: «Whistleblowing europeo y compliance: La Directiva EU de 2019 relativa a la protección de personas que reporten infracciones del Derecho de la Unión», *Diario La Ley*, núm. 9539, 2019, p. 9. Pero, sin duda, iniciativas legislativas como la Directiva (UE) 2019/1937, de 23 de octubre, y su trasposición han contribuido enormemente (por su carácter obligatorio) a la introducción de estos mecanismos de denuncia.

[6] El apartado primero del art. 31 quinquies CP dispone que «Las disposiciones relativas a la responsabilidad penal de las personas jurídicas no serán aplicables al Estado, a las Administraciones públicas territoriales e institucionales, a los Organismos Reguladores, las Agencias y Entidades públicas Empresariales, a las organizaciones internacionales de derecho público, ni a aquellas otras que ejerzan potestades públicas de soberanía o administrativas». Y, por su parte, el apartado segundo del citado precepto establece la siguiente excepción: «En el caso de las Sociedades mercantiles públicas que ejecuten políticas públicas o presten servicios de interés económico general, solamente les podrán ser impuestas las penas previstas en las letras a) y g) del apartado 7 del artículo 33». Por otro lado, el régimen de responsabilidad previsto en los arts. 31 bis y ss. CP se aplica a entidades generalmente lícitas, a diferencia de aquellas otras que forman parte de organizaciones criminales o que se utilizan con carácter instrumental. *Vid.* ampliamente, sobre esta cuestión, Galán Muñoz, A.: «¿Cultura o estructura? ¿esa es la cuestión? La difícil convivencia y coordinación de los dos sistemas de tratamiento penal de las personas jurídicas en el ordenamiento español», *Revista General de Derecho Penal*, núm. 35, 2021, pp. 1-33. Y Abel Souto, M.: «Algunas

mienta comunicativa en tanto en cuanto ello les permitirá, en parte, poder obtener, llegado el caso, una exención absoluta o parcial (atenuación) de la responsabilidad criminal en que pudieran incurrir (o se les atribuya). En este sentido, cabría mencionar que, en relación con el art. 31 bis 2 a 5 CP, no existe ninguna obligación de dotarse de estos mecanismos de prevención de delitos (salvo en el caso de algunos entes como los partidos políticos)[7]. Por lo que su implementación voluntaria lo es a efectos de obtener la exención/atenuación de responsabilidad. No obstante, como veremos en este capítulo, el Anteproyecto de Ley reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción (por la que se transpone la Directiva (UE) 2019/1937 del Parlamento Europeo y del Consejo, de 23 de octubre de 2019, relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión), sí impone la obligación de que determinadas personas jurídicas (no solo privadas) implanten estos mecanismos de «denuncia» corporativa[8]. En este caso, la obligación prevista en este Anteproyecto va acompañada de un catálogo de infracciones (art. 63) y sanciones (arts. 65 y 66) en caso de incumplimiento de algunas de sus previsiones.

En línea con lo anterior, resulta curioso que el proyectado art. 4.1 del citado Anteproyecto aluda a que «Los sistemas internos de información son el cauce preferente para informar sobre las acciones u omisiones previstas en el artículo 2». Ahora bien, mientras no se produzca una modificación de la normativa procesal penal esto en ningún caso puede entenderse como un requisito de procedibilidad, sino, simplemente de una cláusula de fomento del uso «preferente» de estos mecanismos (internos) antes de acudir a las vías convencionales. Pero, nada más.

Precisamente, el Informe del CGPJ sobre el citado Anteproyecto, de 26 de mayo de 2022, destacaba que los arts. 259 y 262 LECrim establecen la obligación de denunciar (con las excepciones contempladas en los

---

discordancias legislativas sobre la responsabilidad criminal de las personas jurídicas en el código penal español», *Revista General de Derecho Penal*, núm. 35, 2021, p. 20 y ss.

[7] *Vid*., sobre esta cuestión, León Alapont, J.: «Partidos políticos y responsabilidad penal de las personas jurídicas: consideraciones en torno a su régimen jurídico y los *compliances programs*», en Matallín Evangelio, Á. (Dir.), *Compliance y prevención de delitos de corrupción*, Valencia, Tirant lo Blanch, 2018, p. 180. Nuestro Código Penal no tipifica como delito la no adopción de modelos de organización y gestión. Si bien, en el Proyecto de Ley Orgánica de reforma del Código Penal de 2013 se llegó a contemplar la introducción (dentro de la nueva sección cuarta bis del capítulo XI del título XIII), de un nuevo artículo 286 seis que castigaba la no adopción de planes de cumplimiento penal. *Vid*., sobre esta cuestión, Gómez Tomillo, M.: *Compliance penal y política legislativa. El deber personal y empresarial de evitar la comisión de ilícitos en el seno de las personas jurídicas*, Valencia, Tirant lo Blanch, 2016.

[8] Así pues, puede haber personas jurídicas que sí queden incluidas en el ámbito subjetivo de aplicación de los arts. 31 bis y ss. CP, pero, que, en cambio, no estén obligadas a adoptar dichos canales de denuncia. Y, viceversa (aunque en menor medida), que, no quedando sometidas al régimen de responsabilidad penal de los arts. 31 bis y ss. CP, sí queden compelidas por la obligación prevista en el Anteproyecto de Ley.

arts. 260, 261 y 263) la perpetración de cualquier delito público ante las autoridades judiciales, fiscales o policiales. Advirtiendo que, a pesar de la simbólica consecuencia que lleva su incumplimiento, «la preexistencia de dichas disposiciones en nuestro ordenamiento jurídico tiene un encaje cuanto menos complejo con la norma europea y el Anteproyecto» (p. 30). Señalándose que, «si bien la denuncia a través de los canales internos o externos es una opción que se proporciona al ciudadano que no resulta per se incompatible con la obligación de denunciar establecida en la LECrim, la consecución real del objetivo de fomento del empleo de estos canales de forma preferente —y en especial, del canal interno— para combatir los incumplimientos del Derecho de la Unión Europea y nacional que se enmarcan en su ámbito de aplicación sí resulta difícilmente conciliable con dicha obligación legal» (p. 31). Por ello, el CGPJ (pp. 31 y 32) valora positivamente que el Anteproyecto de Ley Orgánica de Enjuiciamiento Criminal, si bien mantiene la obligación de denunciar en su artículo 526, prevé a su vez, que «Cuando la noticia de la comisión de un delito cometido en el seno de una entidad del sector público o privado la hubiese dado un funcionario o empleado a través de un procedimiento de denuncia interna, la comunicación del hecho delictivo a las autoridades podrá realizarla el responsable del canal de denuncia sin revelar la identidad del alertador, salvo que fuese especialmente requerido para hacerlo» (artículo 528.6).

Con todo, lo más importante es que, si bien solo determinadas personas jurídicas quedan obligadas por este Anteproyecto (como veremos a continuación), el art. 10. 2 prevé que «Las personas jurídicas del sector privado que no estén vinculadas por la obligación impuesta en el apartado 1 de este artículo podrán establecer su propio sistema interno de informaciones, que deberá cumplir, en todo caso, los requisitos previstos en la presente ley». Esta cláusula viene a despejar, a nuestro juicio, una importante duda, y es que, a falta de una regulación específica en el Código Penal (art. 31 bis 5. 4º CP) sobre canales de denuncia, esta futura Ley será a tales efectos la norma de referencia a la que remitirse y, en consecuencia, los parámetros y disposiciones en ella contenidas serán las que deban tenerse en cuenta a la hora de valorar el cumplimiento (o incumplimiento) del requisito 4º del art. 31 bis 5 CP.

Por último, en el caso de grupos de sociedades o personas jurídicas con varios centros de negocio (o de actuación), podrán adoptarse canales de denuncia «centralizados» (esto es, compartidos) o disponer a nivel individual de éstos.

2. Los canales de denuncia en el marco del *compliance* penal

Como puede observarse, el Código Penal solo establece, en el art. 31 bis 5. 4º, que los modelos de organización y gestión: «impondrán la obligación de informar de posibles riesgos e incumplimientos al organismo

encargado de vigilar el funcionamiento y observancia del modelo de prevención».

En este sentido, cabe advertir que:

a) el mencionado precepto no concreta a través de qué medio se canaliza esa obligación de informar y qué características debe reunir;

b) en ningún momento se alude a la obligación de denunciar, sino a la de «informar»;

c) nada se dice sobre cómo debe gestionarse esa información que se recibe;

d) tampoco se expresa si no gestionar la información o hacerlo indebidamente puede enervar la eficacia eximente del *compliance*; y,

e) el Código Penal no exige que se deba abrir una investigación interna tras la recepción de «información».

Por tanto, en puridad, si nos atenemos al tenor literal del precepto, bastaría con imponer la obligación de informar de posibles riesgos e incumplimientos al órgano de vigilancia[9]. Ahora bien, en nuestra opinión, consideramos razonable que para que se cumpla con el requisito cuarto del art. 31 bis 5 CP deba valorarse, además, la siguiente secuencia lógica[10]:

1) habrá que acreditar que el canal de denuncias se haya implantado y esté en funcionamiento.

2) que reúna, al menos, las siguientes características[11]:

   — deberá determinar quiénes pueden acceder a dicho sistema de denuncias.

   — garantizar la protección del denunciante.

   — ser accesible, esto es, que el procedimiento para reportar un riesgo o incumplimiento del modelo no sea farragoso; y,

   — detallar el proceso de gestión de la denuncia (admisión, estudio, diligencias a practicar, resultado, respuesta, comunicación, etc.).

---

[9] Discrepamos, pues, de la opinión de Puyol Montero, cuando afirma que «expresamente se impone la obligatoriedad del canal de denuncias». *Cfr*. Puyol Montero, J.: *El funcionamiento práctico del canal de compliance «whistleblowing»*, Valencia, Tirant lo Blanch, 2017, p. 105.

[10] León Alapont, J.: *Compliance Penal. Especial referencia a los partidos políticos*, Valencia, Tirant lo Blanch, 2020, pp. 199 y ss.

[11] León Alapont, J.: «*Criminal compliance*: análisis de los arts. 31 bis 2 a 5 y 31 quater CP», *Revista General de Derecho Penal*, núm. 31, 2019, pp. 16-17.

3) que se dé curso a la denuncia, se analice, se valore, y se comunique a los superiores su existencia.

4) decretar la apertura de una investigación interna en caso de que se aprecie que la denuncia es fundada, salvo que no se considere necesaria y se proceda directamente a sancionar.

Respecto de esta última cuestión, como veremos, el Código Penal tampoco contempla expresamente que las personas jurídicas tengan que llevar a cabo investigaciones internas como *conditio sine qua non* para predicar la eficacia eximente de los modelos de organización y gestión. Sin embargo, consideramos una obligación ineludible que, tras la recepción de información sobre posibles riesgos e incumplimientos del *compliance*, la persona jurídica decrete la apertura de la correspondiente investigación interna con la finalidad de esclarecer los hechos objeto de la comunicación[12].

Por su parte, la FGE en su Circular 1/2016, al analizar los requisitos contenidos en el art. 31 bis 5 CP, expresó que «La existencia de unos canales de denuncia de incumplimientos internos o de actividades ilícitas de la empresa es uno de los elementos clave de los modelos de prevención. Ahora bien, para que la obligación impuesta pueda ser exigida a los empleados resulta imprescindible que la entidad cuente con una regulación protectora específica del denunciante (whistleblower), que permita informar sobre incumplimientos varios, facilitando la confidencialidad mediante sistemas que la garanticen en las comunicaciones (llamadas telefónicas, correos electrónicos…) sin riesgo a sufrir represalias»[13].

Asimismo, el CGPJ, en su Informe de 26 de mayo de 2022 (sobre el Anteproyecto de Ley de Protección del Informante), relacionaba estos canales de información con lo dispuesto en los artículos 31 bis. 2, 1ª y 2ª, 31 bis.5, 4ª y 31 quater d) del Código Penal (pp. 17 y 18).

Llegados a este punto, resulta ineludible advertir que, al menos a efectos de la exención o atenuación contemplada en el Código Penal, los riesgos e incumplimientos a los que se refiere el art. 31 bis 5. 4º serán solo aquellos que como tales queden contemplados en el *compliance*. Por tanto, no incluyen (no se extienden) a otras infracciones (de la naturaleza que sean) que no vengan recogidas en el mapa de riesgos a que hace referencia el art. 31 bis 5. 1º CP. Esto es, lo que debe ponerse en conocimiento del responsable del canal es la existencia de un riesgo (probable incumplimiento) o de una actual trasgresión de algunas de las disposiciones del

[12] León Alapont, J.: «Retos jurídicos en el marco de las investigaciones internas corporativas: a propósito de los *compliances*», *Revista Electrónica de Ciencia Penal y Criminología*, núm. 22-04, 2020, p. 4.

[13] Circular 1/2016, de 22 de enero, sobre la responsabilidad de las personas jurídicas conforme a la reforma del Código Penal efectuada por Ley Orgánica 1/2015, p. 45.

programa en relación con algunas de las actividades previamente identificadas como peligrosas (potencialmente delictivas).

Naturalmente, es posible que la realización del *risk mapping* no se haya efectuado de la manera adecuada, presente importantes deficiencias, o hayan surgido nuevos riesgos con posterioridad a la valoración inicial. Por ello, no puede excluirse la posibilidad de que se reporten hechos aparentemente «sospechosos» de ser constitutivos de delito en relación con actividades que pueden no estar recogidas en el mapa de riesgos y que sean igualmente imputables a la persona jurídica.

Otra cosa es que, más allá de esta previsión, se decida que el canal de denuncias deba configurarse de forma que no solo reciba y atienda comunicaciones de índole penal, sino, también, de otra naturaleza.

De igual modo, los canales de denuncia pueden ser de gran ayuda para la comunicación de posibles conductas delictivas en operaciones de fusión, absorción o escisión (las cuales no extinguen la responsabilidad penal, sino que la transmiten a la entidad o entidades resultantes); y, muy especialmente, de las acontecidas con anterioridad a la culminación de tales procesos.

Por último, también en este ámbito concreto de los canales de denuncia existen estándares como la UNE 19601:2017 sobre *Sistemas de gestión de compliance penal. Requisitos con orientación para su uso* o, más específicamente, la UNE-ISO 37002:2021 sobre *Sistemas de gestión de la denuncia de irregularidades. Directrices*. En relación con esta última, se ha afirmado que se trata de «un referente de primer orden, tanto para las organizaciones y sus asesores en el momento de implantar el sistema, como para los abogados, jueces y fiscales en caso de que alguna persona jurídica sea procesada penalmente y su modelo de prevención deba ser sometido a revisión a los efectos de valorar la responsabilidad penal de dicha entidad. Si bien la ISO no es un texto de obligado seguimiento, no cabe duda de que el prestigio de la entidad que ha formulado este estándar constituye una garantía de que, en caso de aplicarse correctamente, la organización sometida a escrutinio penal deberá ser vista favorablemente por las autoridades, al menos en este punto concreto del modelo de prevención»[14]. Por el contrario, debemos mostrar nuestro frontal rechazo a la confianza ciega depositada en este tipo de previsiones, pues, tales referencias no son normativas, sino un conjunto de pautas, parámetros y criterios elaborados por determinadas entidades privadas que, bajo ninguna circunstancia, pueden calificarse como texto legal. En este sentido, no llegamos a entender la influencia que entidades privadas como, por ejemplo, ISO o AENOR, tienen cada vez más en el ámbito «normativo» y,

[14] Ragués I Vallés, R.: «Un nuevo avance en la estandarización de los modelos de prevención de delitos: la ISO 37002 sobre gestión de sistemas de denuncia», *La Ley Compliance penal*, núm. 7, 2021, p. 6.

muestra de ello es, el sector del compliance. Por tanto, sin despreciar en modo alguno la importante labor que estas entidades realizan, consideramos que se les da un protagonismo sobredimensionado, pues, al fin y al cabo, no son ni legislador, ni jueces, ni parte de la Administración Pública.

3. Aspectos prácticos

3.1. ¿Quién puede denunciar?

Al contrario de lo que han defendido algunos autores, como por ejemplo Ragués i Vallés, el canal de comunicación no solo debe estar abierto para denuncias de empleados, esto es un error de planteamiento[15]. Como también lo es pensar que «resulta más complejo, sin embargo, hablar de *whistleblowing* cuando la denuncia proviene de algún directivo o administrador, pues generalmente a ellos les corresponde adoptar e implementar los canales de denuncia interna y los programas de cumplimiento legal»[16]. Excluir a cualquier persona integrante de la organización de la posibilidad de acceder al canal de denuncias no sólo restará eficacia a este mecanismo, sino que además debería impedir considerar este requisito (al menos en su plenitud) y negar la exención absoluta de responsabilidad penal de la persona jurídica[17].

Ahora bien, tampoco compartimos la tesis de que el canal de denuncias no deba tener límites al conocimiento o denuncia de irregularidades vinculadas a las actividades de la entidad, de forma que la persona jurídica pudiera conocer el incumplimiento de su modelo de prevención penal[18]. Así pues, el canal debe estar accesible a cualquier persona que colabore o hubiese colaborado con la organización, o que tenga o hubiese tenido relación con la misma. Lo que es evidente, es que no puede exigirse a una persona jurídica que el canal de denuncias también esté abierto a cualquier persona «ajena» o sin ningún tipo de vinculación con ésta[19].

---

[15] *Cfr.* Ragués I Vallés, R.: «Denuncias de los trabajadores («whistleblowing»)», en Ayala Gómez, I. Y Ortiz De Urbina Gimeno, I. (Coords.): *Penal económico y de la empresa*, Madrid, Francis Lefebvre, 2016, p. 201.

[16] Gimeno Beviá, J.: *Compliance y proceso penal. El proceso penal de las personas jurídicas*, Cizur Menor, Thomson Reuters-Aranzadi, 2016, p. 74.

[17] León Alapont, «*Criminal compliance…*», *op. cit.*, p. 16.

[18] Díaz Aldao, M. y Hernández Pérez, E.: «Las investigaciones internas del modelo de prevención penal», en Gómez-Jara Díez, C. (Coord.): *Persuadir y Razonar: Estudios Jurídicos en Homenaje a José Manuel Maza Martín. Tomo II*, Cizur Menor, Thomson Reuters-Aranzadi, 2018, pp. 993.

[19] León Alapont, «*Criminal compliance…*», *op. cit.*, p. 16.

En este sentido, podría pensarse por ejemplo en extender la posibilidad de denunciar también a socios, afiliados, a proveedores, etc. Incluso, a pesar de lo dicho anteriormente, también un vecino puede observar «movimientos» sospechosos en la sucursal de enfrente de su casa (y ponerlo en conocimiento de la empresa); o, un cliente que escucha conversaciones o presencia comportamientos «extraños» de algún empleado.

Por otro lado, a juicio de algún autor, en el caso concreto de un partido político (aunque resulta de aplicación a otro tipo de organizaciones como sindicatos, asociaciones, etc.) los canales internos de denuncia «deberían estar reservados para los integrantes, directivos o empleados de la organización, y no a los afiliados de la misma que, en estos casos, actuarían como personas ajenas a ella, con las mismas características de cualquier ciudadano que denuncie las prácticas ilícitas cometidas por las personas físicas integrantes del partido político»[20]. Sin embargo, a nuestro juicio, no vemos obstáculo alguno para ello, pues, como ya hemos manifestado más arriba, incluso, sería altamente aconsejable que así fuere[21].

3.2. ¿Qué se puede denunciar?

Como advertimos más arriba, el requisito cuarto del art. 31 bis 5 CP alude a la obligación de informar sobre posibles «*riesgos e incumplimientos*» (actuales o inminentes), se entiende, de carácter delictivo. Con todo, si bien ésta debe ser la función principal del canal de denuncias, éste puede emplearse igualmente para otro tipo de comunicaciones como las que destacamos a continuación[22]:

a) plantear dudas sobre el funcionamiento de determinados aspectos del programa de cumplimiento;

b) consultar sobre la legalidad de determinadas operaciones;

c) comunicar cualquier tipo de incidencia;

d) presentar cualquier tipo reclamación;

e) realizar sugerencias de reforma de algunos elementos del *compliance*;

---

[20] Maza Martín, J. M.: *Delincuencia electoral y responsabilidad penal de los partidos políticos*, Las Rozas, La Ley-Wolters Kluwer, 2018, p. 456.

[21] León Alapont, J.: *La responsabilidad penal de los partidos políticos*, Valencia, Tirant lo Blanch, 2019, p. 522.

[22] De este mismo parecer, Casanovas Ysla, A.: «La norma UNE 19601 y los requisitos del Código Penal», en Gómez-Jara Díez, C. (Coord.): *Persuadir y Razonar: Estudios Jurídicos en Homenaje a José Manuel Maza Martín. Tomo II*, Cizur Menor, Thomson Reuters-Aranzadi, 2018, p. 911. Y Puyol Montero, *El funcionamiento…*, *op. cit.*, pp. 15 y 185.

f) reportar la detección de nuevos riesgos;

g) proponer acciones de mejora; y,

h) cualesquiera otras circunstancias de naturaleza análoga a las anteriores.

Y, como también dijimos, los canales de denuncia pueden emplearse para la puesta en conocimiento de otro tipo de infracciones que no sean de naturaleza penal (como las de carácter administrativo, tributario, laboral, etc.). O, incluso, aun siendo delictivas, que versen sobre delitos no atribuibles a la persona jurídica, o en los que ésta aparezca como víctima (como en el caso de una administración desleal, una estafa, etc.). Pudiéndose igualmente informar de hechos que pudiesen desencadenar en una responsabilidad civil subsidiaria (art. 120.4º CP) o en una participación a título lucrativo (art. 122 CP).

Sin olvidar que las denuncias también pueden ir referidas a violaciones del Código Ético o de buena conducta. De forma que, igualmente podrían comunicarse incumplimientos de los valores, principios, o pautas que la persona jurídica haya decidido establecer en su seno.

Por último, sí que consideramos conveniente diferenciar entre lo que podrían considerarse «denuncias» (referidas a hechos, conductas, comportamientos, etc.), de las «reclamaciones» que, por ejemplo, puedan presentarse ante una empresa por defectos en el producto o servicio, por el trato o atención dispensada al cliente, etc. (más de naturaleza civil o mercantil).

Centrándonos, a continuación, únicamente en la vertiente penal del canal de denuncias, habría que tener en cuenta que la responsabilidad penal de las personas jurídicas puede originarse por:

a) acciones u omisiones (propias o impropias);

b) delitos dolosos e imprudentes;

c) en grado de consumación o tentativa (acabada e inacaba);

d) cuando la persona física actúa no solo como autor (directo, mediato, o coautor), sino también cuando lo hace en calidad de partícipe (inductor, cooperador necesario y cómplice); y,

e) actos preparatorios punibles.

Pero, la principal cuestión que aquí se suscita es si las personas sujetas al canal de denuncias tienen la obligación de revelar cualquier clase de incumplimiento por mínimo e inconsistente que sea, e independientemente de la gravedad y del perjuicio real o potencial que se pueda causar a la organización. A nuestro parecer, y en los términos expuestos hasta el momento, la denuncia debe versar sobre cualquier posible riesgo de comisión delictiva o incumplimiento (ya producido) de las disposiciones

del *compliance* que pueda acabar generando responsabilidad penal para la entidad. Así, un plan de prevención de delitos que estableciese un listado elaborado por la propia persona jurídica delimitando los supuestos en que cabría denunciar, debería reputarse, a nuestro juicio, no apto para la exención[23]. Lo cual no obsta para que, posteriormente, los parámetros arriba enunciados se tuvieren en consideración a la hora de dar curso o no a la denuncia o, en su caso, llegar a «archivarla». Pero, en ningún caso, utilizarlos como elementos para limitar *ab initio* la facultad de denuncia interna.

Cuestión distinta será que a la hora de sancionar el incumplimiento de la obligación de «informar» se establezca una suerte de catálogo que recoja aquellas situaciones que se considerarán infracciones del código disciplinario, atendiendo a una serie de criterios como podrían ser los siguientes:

— La gravedad del incumplimiento o posible riesgo detectado.

— La repercusión (económica, reputacional, o de cualquier otra clase).

— La posición que la persona física denunciada ocupe en la estructura organizativa de la persona jurídica.

— Etc.

En definitiva, los supuestos de inobservancia de la obligación de denunciar han de interpretarse de manera restrictiva[24].

3.3. ¿Qué consecuencias puede generar, en su caso, no denunciar estando «obligado» a ello?

En primer lugar, cabría advertir que en el caso del art. 31 bis 5. 4º CP se trata de una «obligación» (la de denunciar) *sui generis*, pues, en realidad la puede establecer la empresa (o no) para que en un momento dado ello puede acreditarse como parte del modelo de compliance y así optar a la exención o atenuación de responsabilidad penal. Por tanto, no es ninguna obligación legal. En la actualidad, fuera del *corporate compliance*, debe recurrirse a la regulación sectorial para conocer si existe algún tipo de obligación de denunciar determinadas conductas.

En cualquier caso, como sostiene Goñi Sein, la delación obligatoria conduce a resultados poco satisfactorios, pues, implica instaurar prácti-

[23] León Alapont, «*Criminal compliance…*», *op. cit.*, p. 17.

[24] *Cfr*. Goñi Sein, J. L.: «Programas de cumplimiento empresarial (*compliance programs*): aspectos laborales», en Mir Puig, S.; Corcoy Bidasolo, M. Y Gómez Martín, V.: *Responsabilidad de la empresa y compliance. Programas de prevención, detección y reacción penal*, Montevideo-Buenos Aires, B de F, 2013, p. 401.

camente una estructura cuasi policial en la organización[25]. En este sentido, consideramos que lo preferible hubiere sido que la obligación a la que alude el requisito cuarto del art. 31 bis 5 CP se circunscribiese a la implantación de dichos canales (cosa que, en sentido estricto, como ya expusimos, no exige el precepto), de forma que la decisión de denunciar fuere totalmente voluntaria. Con todo, el legislador no valoró este aspecto e impuso la obligación de «informar» para aspirar a obtener la exención, desestimando otras vías como el establecimiento de políticas de «incentivos» o recompensas a los *whistleblowers*, tan frecuentes en otras latitudes en la lucha contra la criminalidad corporativa.

Dejando atrás este debate, debe tenerse en cuenta que, por otra parte, el citado precepto emplea los términos *posibles riesgos e incumplimientos* como objeto de la «comunicación». Por tanto, ni sólo se refiere a conductas delictivas (incumplimientos), ni sólo se refiere a hechos consumados (posibles riesgos). La primera consecuencia de ello es que a ojos del denunciante lo que habrá es una «irregularidad». Así las cosas, que la acción u omisión quepa calificarla como delictiva, constitutiva de una infracción administrativa, o un incumplimiento del *compliance* será algo que trascienda del juicio que éste pueda hacer, si es el caso.

La obligación de informar de posibles riesgos e incumplimientos es uno de los principales aspectos en los que la acción formativa deberá incidir con especial ahínco[26].

Sobre todo, porque, en ningún momento el requisito cuarto del art. 31 bis 5 CP impone la obligación de sancionar el incumplimiento de dicho mandato. Llegados a este punto, convendría recordar que la renuencia de un empleado a denunciar en el canal interno de la empresa solo podrá castigarse cuando así venga establecido en una ley (como pudiera ser el Estatuto de los Trabajadores o una norma como el Anteproyecto); en el convenio colectivo; o, en un contrato de trabajo laboral, o mercantil (como en el caso del personal de alta dirección). Y, en igual sentido, cuando se trate de otros sujetos cabrá acudir a otra clase de normas reglamentarias como puedan ser los estatutos de un partido político o sindicato (con respecto de sus afiliados), u otras «disposiciones» o acuerdos como en casos de ONG's, asociaciones, fundaciones, etc. (respecto de sus miembros). Por tanto, si bien a juicio de algún autor, lo lógico sería que el incumplimiento de la obligación de denunciar quedase recogido en el respectivo régimen sancionador del *compliance*[27], ello solo será posible

---

[25] *Cfr*. Goñi Sein, J. L.: «Criminalidad de empresa, mecanismos de denuncia o *whistleblowing* y protección de datos», en AA.VV: *Derecho de la empresa y protección de datos*, Cizur Menor, Thomson Reuters-Aranzadi, 2008, p. 40.

[26] León Alapont, «*Criminal compliance…*», *op. cit.*, p. 13.

[27] Así, para Palma Herrera, el incumplimiento de dicha obligación tendría que llevar aparejada la correspondiente sanción. *Vid*., Palma Herrera, J.M.: «Presupuestos jurídico-penales de la responsabilidad penal de los entes corporativos y del sistema de «complian-

en caso de que las disposiciones del compliance constituyesen fuente de obligaciones porque así se pactare o se estableciese en una disposición normativa que remitiese a ellas. De lo contrario, a nuestro juicio, quedarían sin cobertura jurídica o legal.

Con todo, el mandato que instaura el requisito quinto del art. 31 bis 5 CP (la de imponer la obligación de informar) presenta otra serie de limitaciones. En el supuesto concreto que aquí se dilucida, debe tenerse especialmente en cuenta que, llegado el caso, la facultad sancionadora de la persona jurídica sólo podrá proyectarse *ad intra*, esto es, respecto de las personas sobre las que ésta ejerza influencia, de forma que no alcanzaría a personas «externas» (como sería el caso de todas aquellas a las que se hubiera posibilitado el acceso al canal de denuncias interno sin pertenecer a aquélla) por cuanto en estos casos no sería viable exigir dicho cumplimiento de forma coercitiva. En tales casos (piénsese, por ejemplo, en una empresa suministradora), y aun cuando podrían incluirse cláusulas contractuales al respecto que contemplaran dicha obligación, en caso de incumplimiento se podrían adoptar otra serie de medidas como, por ejemplo, rescindir la relación mercantil[28].

En todo caso, como destaca Ragués i Vallés, «razones evidentes de proporcionalidad deberían impedir tratar con la misma severidad al trabajador no denunciante que al empleado infractor»[29].

3.4. El eterno debate: ¿canal de denuncias anónimo o confidencial?

La persona jurídica puede optar entre diversas modalidades a la hora de proteger la identidad del denunciante.

Así, por ejemplo, puede implantar un canal de denuncias anónimo. A este respecto, el apartado primero del art. 24 LOPDGDD (relativo a los sistemas de información de denuncias internas) establece que: «será lícita la creación y mantenimiento de sistemas de información a través de los cuales pueda ponerse en conocimiento de una entidad de Derecho privado, incluso anónimamente, la comisión en el seno de la misma o en la actuación de terceros que contratasen con ella, de actos o conductas que pudieran resultar contrarios a la normativa general o sectorial que le fuera aplicable. Los empleados y terceros deberán ser informados acerca de la existencia de estos sistemas de información».

---

ces»", en Palma Herrera, J. M. Y Aguilera Gordillo, R.: *Compliances y responsabilidad penal corporativa*, Cizur Menor, Thomson Reuters-Aranzadi, 2017, pp. 58-59.

[28] León Alapont, *La responsabilidad…*, *op. cit.*, p. 522.

[29] Ragués I Vallés, Denuncias…», *op cit.*, p. 202.

Además, tanto la Directiva europea como el Anteproyecto prevén dicha posibilidad.

Por otro lado, puede garantizarse la confidencialidad del denunciante. Así, el art. 24.3 LOPDGDD expresa que: «deberán adoptarse las medidas necesarias para preservar la identidad y garantizar la confidencialidad de los datos correspondientes a las personas afectadas por la información suministrada, especialmente la de la persona que hubiera puesto los hechos en conocimiento de la entidad, en caso de que se hubiera identificado».

En relación con esta cuestión, el Anteproyecto de LECrim de 2020 recoge en su art. 528.6 que «Cuando la noticia de la comisión de un delito cometido en el seno de una entidad del sector público o privado la hubiese dado un funcionario o empleado a través de un procedimiento de denuncia interna, la comunicación del hecho delictivo a las autoridades podrá realizarla el responsable del canal de denuncia sin revelar la identidad del alertador, salvo que fuese especialmente requerido para hacerlo».

Pero, también puede abogarse por un sistema mixto, esto es, que la organización ofrezca ambas posibilidades.

El canal de comunicación anónimo presenta, sin duda, algunos inconvenientes[30]. Así, a título ilustrativo, podrían citarse los siguientes:

— El hecho de presentar una denuncia anónima no impide que, por la clase de información que se aporte, los receptores de la misma acierten al conjeturar sobre quién presentó la denuncia, por lo que puede acabar descubriéndose la identidad del informante.

— Es más difícil realizar una investigación interna si no se puede contactar con el denunciante para que se pronuncie sobre algún aspecto que requiera algún tipo de aclaración por su parte, etc., (salvo que aporte pruebas o información bastante precisa).

[30] Especialmente crítico se muestra en este sentido Galán Muñoz, para quien directamente los canales de denuncia anónimos son inconstitucionales por no superar el triple juicio de idoneidad, de necesidad y de proporcionalidad en sentido estricto. *Vid.* ampliamente, Galán Muñoz, A.: «Whistleblowing anónimo y compliance penal tras la aprobación de la Ley Orgánica 3/2018, de Protección de Datos personales y de garantía de los derechos digitales: una decisión político-criminal a revisar», en Colomer Hernández, I. (Dir.): *Uso y cesión de evidencias y datos personales entre procesos y procedimientos sancionadores o tributarios*, Cizur Menor, Thomson Reuters-Aranzadi, 2019, pp. 254-261. *Vid*. también, sobre los riesgos que entrañan este tipo de denuncias anónimas, Gimeno Beviá. J.: «Whistleblowing y proceso penal: una lectura desde las garantías procesales», en Olaizola Nogales, I.; Sierra Hernaiz, E. Y López López, H. (Dirs.): *Análisis de la Directiva UE 2019/1937, Whistleblower desde las perspectivas penal, procesal laboral y administrativo-financiera*, Cizur Menor, Thomson Reuters-Aranzadi, 2021, p. 175.

— El anonimato puede favorecer que se presenten más denuncias de tipo difamatorio (y, por ende, que resulten más proclives a infringir derechos como el honor o la intimidad).

— Puede verse comprometido el derecho de defensa[31].

— El ambiente en el seno de la organización puede deteriorarse si sus integrantes piensan que a través del sistema se pueden presentar denuncias anónimas sobre ellos en cualquier momento.

Pero, también un canal confidencial de denuncias presenta problemas. El principal, sin duda, el recelo que genera el hecho de que el responsable del canal u otros tengan acceso a la identidad del denunciante. Y, asociado a lo anterior, el temor a posibles represalias (despido, etc.). Esto último resulta especialmente preocupante en algunos tipos de personas jurídicas; como, por ejemplo, los partidos políticos, en los que, como pone de manifiesto Maroto Calatayud, se sanciona gravemente en sus estatutos y normas de organización interna, a través de diversas fórmulas (desobediencia, revelación de secretos, difamación) este tipo de conductas[32].

Personalmente, sin tener una preferencia clara por uno u otro tipo de sistemas, sí que consideramos que o bien se configura un canal confidencial lo más garantista posible con la reserva de la identidad del denunciante y sus derechos (que pudiera decaer ante un posible proceso penal cuando así se estimase judicialmente); o, de lo contrario, la solución debiera pasar por establecer un canal de denuncias anónimo (con filtros sobre la seriedad o no de las informaciones, y otro tipo de precauciones para evitar determinados riesgos)[33].

Aunque la vía mixta (o alternativa) podría ser, en ocasiones, de utilidad. Como, por ejemplo, en aquellos supuestos en los que, partiéndose de una denuncia anónima, se decide y se anuncia (no siendo posible la notificación personal dado el anonimato) que el procedimiento de averiguación (o investigación interna) no continue en tanto que el *whistleblower* no se identifique, o no aporte la documentación que se le requiera, etc.

Con todo, una vez más, creemos que se cae en el error de considerar estos mecanismos de denuncia interna como una suerte de instrumento de investigación policial/judicial paralelo al institucional (u oficial). De

[31] En puridad, como sabemos, solo podemos entender conculcado el derecho de defensa cuando estemos en el ámbito de un proceso judicial; o, a lo sumo, en un procedimiento sancionador. Queremos con ello advertir que, según la clase de incumplimiento que se reporte, puede que ni tan siquiera quepa hablar en esos términos.

[32] Maroto Calatayud, M.: *La financiación ilegal de los partidos políticos: un análisis político-criminal*, Madrid, Marcial Pons, 2015, p. 336.

[33] A favor del anonimato, Aránguez Sánchez, «El diseño de programas…», *op. cit*., p. 16.

ahí que, en nuestra opinión, toda impregnación de carácter inquisitorio a este tipo de herramientas pueda resultar en la mayoría de los casos desmedida. Discusión que trasladada al prolijo debate sobre la implantación de canales anónimos o confidenciales puede acabar resultando, en consecuencia, exagerada.

4. Los diferentes escenarios que se le plantean al denunciante, al receptor directo de la comunicación y a la persona jurídica involucrada

El requisito cuarto del art. 31 bis 5 CP no ofrece dudas al respecto: las denuncias se tienen que dirigir *al organismo encargado de vigilar el funcionamiento y observancia del modelo de prevención*. En clara alusión al órgano de cumplimiento (*compliance officer*).

Naturalmente, los incumplimientos que consistan únicamente en violaciones del modelo de *compliance* (de sus disposiciones), siempre que no produzcan ninguna consecuencia jurídica para la empresa, deberán dirigirse de forma exclusiva al responsable del canal.

Ahora bien, cuando se trate de otra clase de hechos o conductas (de naturaleza penal o no) que puedan suponer una infracción del ordenamiento jurídico; y, según se hayan producido fuera o dentro del *compliance*, las alternativas que se presentan son mayores. Por ello, a continuación, expondremos algunos de esos diversos escenarios.

ESCENARIO A. El denunciante/*whistleblower*:

- Opción 1: *pone los hechos directamente en conocimiento de la policía, fiscalía, o juez solo cuando rezumen carácter delictivo.*

  Premisa 1: lo hace por miedo a la eventual responsabilidad penal en que pueda incurrir si no denuncia ante las respectivas autoridades. Con todo:

  a) El art. 259 LECrim contempla un deber de denunciar «simbólico»[34]: «El que presenciare la perpetración de cualquier delito público está obligado a ponerlo inmediatamente en conocimiento del Juez de instrucción, de paz, comarcal o municipal o funcionario fiscal más próximo al sitio en que se hallare, bajo la multa de 25 a 250 pesetas». Y, aunque la LECrim atribuye a la denuncia el carácter de obligación, solo es coercible el incumplimiento cuando se trata de funcionarios públicos respec-

[34] Ragués I Vallés, «Denuncias…», *op cit.*, p. 201.

to de hechos conocidos en el ejercicio de sus cargos (art. 262 LECrim)[35].

b) el hecho de «tener conocimiento de la comisión de un delito» no es encubrimiento sino se realizan las conductas típicas del art. 451 CP.

c) resulta difícil creer que estuviésemos ante un delito de omisión del deber de impedir delitos o promover su persecución (art. 450 CP):

> «1. El que, pudiendo hacerlo con su intervención inmediata y sin riesgo propio o ajeno, no impidiere la comisión de un delito que afecte a las personas en su vida, integridad o salud, libertad o libertad sexual, será castigado con la pena de prisión de seis meses a dos años si el delito fuera contra la vida, y la de multa de seis a veinticuatro meses en los demás casos, salvo que al delito no impedido le correspondiera igual o menor pena, en cuyo caso se impondrá la pena inferior en grado a la de aquél.
>
> 2. En las mismas penas incurrirá quien, pudiendo hacerlo, no acuda a la autoridad o a sus agentes para que impidan un delito de los previstos en el apartado anterior y de cuya próxima o actual comisión tenga noticia».

Entre otras cosas, porque la obligación de impedir o promover su persecución se predica sólo de determinados delitos; y, no se contempla la obligación de denunciar infracciones ya consumadas.

Premisa 2: lo hace ante el intento fallido de denuncia interna, ante la respuesta negativa recibida por parte de la empresa; o, ante la imposibilidad de denunciar en otros canales de comunicación públicos, o ante su rechazo.

- Opción 2: *acude a organismos (públicos o privados) específicos, receptores de denuncias en ámbitos concretos o especializados, cuando no se trate de una infracción de naturaleza penal.*
  - — De naturaleza administrativa: la CNMV, la CNMC, el SEPBLAC, el Banco de España, la Agencia de Protección de Datos, etc.
  - — De naturaleza civil: organizaciones de consumidores.
  - — De naturaleza tributaria: la AEAT.
  - — Otros: la inspección de trabajo, de sanidad, etc.

[35] Gimeno Beviá, *Compliance y proceso…*, *op. cit.*, p. 92.

- Opción 3: *recurre a canales de denuncia externos (de Administraciones Públicas), como, por ejemplo, las Agencias Antifraude/anticorrupción.*

  Piénsese, a título ilustrativo, en materia subvenciones, de contratación pública, de medio ambiente, urbanismo, etc.

- Opción 4: *denuncia ante la Autoridad Independiente de Protección del Informante u organismos autonómicos equivalentes.*

  El art. 16 del Anteproyecto de Ley reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción, prevé que toda persona física puede informar ante este organismo público de cualesquiera acciones u omisiones incluidas en el ámbito de aplicación de esta ley (directamente o previa comunicación al correspondiente canal interno).

  Por su parte, el art. 24 del citado Anteproyecto establece el reparto competencial entre la Autoridad nacional y las autonómicas. Siendo la primera competente cuando la comunicación efectuada se localice en más de una comunidad autónoma; y, las segundas, cuando se circunscriban a su territorio autonómico.

- Opción 5: *denuncia ante el canal interno*.

  Dado que no se puede evitar que el denunciante recurra a otros medios y no al canal de comunicación de la persona jurídica, es de suma importancia establecer una política de incentivos para que se «denuncien» internamente los incumplimientos que no solo comporten una contravención de las disposiciones «organizativas» del compliance, sino también aquellos que supongan una infracción del ordenamiento jurídico. Y no sólo nos estamos refiriendo a sancionar la trasgresión de dicha obligación o a garantizar el anonimato o confidencialidad del informante frente a posibles represalias, sino a incentivos que pueden ser económicos (a modo de recompensa) o de otro tipo (políticas de promoción, mejora de las condiciones laborales, etc.)[36]. Por tanto, insistimos en que resulta esencial para los intereses de la organización que ésta consiga que se denuncie a través del canal y no se acuda a las autoridades o medios de comunicación.

  Dicho de otro modo, el canal de denuncias interno debería ser el cauce preferente a la hora de informar sobre cualquier tipo de «riesgos» e «incumplimientos» de los modelos de organización.

[36] Esto último será posible en el caso de que la persona jurídica haya establecido un canal de comunicación confidencial y no anónimo.

- Opción 6: *lleva a cabo un acto de comunicación pública*.

  a) denuncia ante los medios de comunicación.

  En estos casos, como indica Gimeno Beviá, «debe existir cierta relevancia social, tanto de la notoriedad de la persona jurídica denunciada como de la conducta irregular para resultar atractiva a los ojos de los medios que lo difunda»[37].

  b) realiza lo que el Anteproyecto de Ley reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción denomina «revelación pública» (art. 27), esto es, una puesta a disposición del público de información.

ESCENARIO B. El responsable o los responsables del canal:

- Opción 1: *pone los hechos (aparentemente delictivos) directamente en conocimiento de la policía, fiscalía, o juez*.

  Damos por reproducidos los mismos argumentos que empleamos en el anterior escenario. Si bien, quisiéramos manifestar de nuevo nuestra oposición a argumentos tan tajantes como el que a continuación se refleja: «cuando el tratamiento de la información suponga una auténtica denuncia de un delito, en ese caso, *los responsables del canal* deben ponerlo en conocimiento de las autoridades competentes para que investiguen el delito, sino quieren verse inmiscuidos en un proceso penal en calidad de encubridores del delito»[38].

- Opción 2: *acude a organismos (públicos o privados) específicos, receptores de denuncias en ámbitos concretos o especializados, cuando no se trate de una infracción de naturaleza penal.*

- Opción 3: *recurre a canales de denuncia externos (de Administraciones Públicas), como, por ejemplo, las Agencias Antifraude/anticorrupción.*

- Opción 4: *denuncia ante la Autoridad Independiente de Protección del Informante u organismos autonómicos equivalentes.*

  Aunque esta, como las dos anteriores, sea también una alternativa para el responsable del canal de denuncias, lo deseable sería que no recurriese a ella, y procediera a comunicar internamente los hechos de los que haya tenido conocimiento.

[37] *Idem*.

[38] Etxeberria Bereziartua, E.: ««Whistleblowing» o canales de denuncia: La garganta profunda de las empresas», *Diario La Ley*, núm. 9342, 2019, p. 4.

- Opción 5: *da traslado de la denuncia a la dirección/órgano de gobierno de la persona jurídica para que éste decida cómo proceder.*

  Esta debería ser, en principio, la reacción que cabría esperar del *compliance officer*.

  Además, debe tenerse en cuenta que, como vimos, la condición 4ª del art. 31 bis 2 CP exige que no se haya producido una omisión o un ejercicio insuficiente de las funciones de supervisión, vigilancia y control por parte del órgano al que se refiere la condición 2ª. Y, entre ellas, cabe incluir la de reportar al órgano de dirección (o de gobierno) de la persona jurídica tales comunicaciones.

- Opción 6: la posibilidad de realizar un *acto de comunicación pública* (por ejemplo, a través de los medios de comunicación) resulta, en principio, remota (aunque lógicamente no descartable).

ESCENARIO C. La persona jurídica:

- Opción 1: *toma la decisión de «autodenunciarse» habiendo aparentemente indicios de delito.*

  Esta es una alternativa que a la persona jurídica se le planteará, sobre todo, cuando haya una alta probabilidad de ser condenada: porque hay indicios suficientes de delito, porque se dan las circunstancias previstas en el art. 31 bis 1 CP, o porque no dispone de *compliance* o no de uno idóneo.

  Premisa 1: lo hace con la finalidad de obtener las atenuantes de confesión, colaboración o reparación del daño previstas en el art. 31 *quater* CP.

  La Fiscalía General del Estado, en relación con esto último, realiza afirmaciones, a nuestro modo de ver, insostenibles[39]:

  a) «(…) detectada la conducta delictiva por la persona jurídica y puesta en conocimiento de la autoridad, deberán solicitar la exención de pena de la persona jurídica (…)».

  A nuestro juicio, la puesta «en conocimiento de» (confesión) no puede llegar a producir la exención porque, sencillamente, no se alude a ello en el Código Penal. Sólo se concibe como atenuante.

  Y, al contrario, no confesar no puede perjudicar que se aplique la eximente, pues, una opción desechable sería la de reconducirlo por la vía de la atenuación por «acreditación parcial» del modelo.

[39] Circular de la Fiscalía General del Estado 1/2016, de 22 de enero, sobre la responsabilidad de las personas jurídicas conforme a la reforma del Código Penal efectuada por Ley Orgánica 1/2015, pp. 53-55.

En consecuencia, si a algunos esta situación les genera cierta perplejidad, lo que debe proponerse es la introducción en el Código Penal de una cláusula que impida exonerar de responsabilidad a la persona jurídica cuando, habiendo ésta detectado un delito, no lo comunique a las autoridades. Lo que no cabe es inventarse cosas que la ley no dice. Aunque, personalmente, nos mostramos en contra de una solución como la aquí reseñada, pues, no corresponde a la persona jurídica determinar si hay o no delito, esa valoración la tienen que hacer (tras la práctica de la prueba o en fase de diligencias preliminares) los jueces y tribunales.

b) «(…) Del mismo modo, la restitución, la reparación inmediata del daño, la (…) pueden permitir llegar a la exención de la pena».

Con esta aseveración, la Fiscalía, una vez más, se aparta del tenor de la ley. En lo que vendría a suponer una más que manifiesta trasgresión del principio de legalidad que nos preocupa.

c) «(…) Operarán en sentido contrario el retraso en la denuncia de la conducta delictiva o su ocultación y la actividad obstructiva o no colaboradora con la justicia».

Esto, a nuestro juicio, constituye una interpretación intolerable porque:

1) El retraso en la denuncia de la conducta delictiva, su ocultación y la no colaboración con la justicia son «actitudes» amparadas por determinados derechos fundamentales de los que también gozan las personas morales, por tanto, no pueden operar en su contra; y,

2) La actividad obstructiva, que puede llegar a ser constitutiva de delito, no puede atribuirse a la persona jurídica (*numerus clausus*).

Premisa 2: decide autodenunciarse dado que los delitos que se le atribuyen no llevan aparejada una sanción excesiva; y, así, dar una imagen de «buen ciudadano corporativo» a la vez que disminuir los efectivos negativos sobre su reputación.

Premisa 3: lo hace con la intención de llegar a un acuerdo de conformidad con la Fiscalía lo más benévolo posible.

- Opción 2: *denuncia los hechos aparentemente delictivos acaecidos en su seno.*

Premisa 1: porque el supuesto delito cometido no es de los que se pueden imputar a una persona jurídica.

Premisa 2: porque considera que la responsabilidad penal debe exigirse únicamente a alguna de las personas físicas de la letra a) o b) del art. 31 bis 1 CP.

Premisa 3: porque estima que dispone de un compliance que le va a exonerar de responsabilidad (o ver atenuada la misma); y, sobre todo, porque va a poder demostrar que lo que hubo fue una elusión fraudulenta del modelo.

- Opción 3: *tratándose de infracciones de naturaleza distinta a la penal (administrativa, tributaria, laboral, civil, etc.), decide «denunciarse» ante los organismos públicos o privados que existan a tales efectos.*

  En estos casos, la «autodenuncia» puede ser útil para: evitar un procedimiento de sanción; disminuir su impacto; evitar otro tipo de consecuencias (más allá de las económicas) que puedan paralizar su actividad; etc.

- Opción 4: *no se denuncia a sí misma*.

  En primer lugar, debemos advertir que una cosa es que la persona jurídica no dé trámite o no resuelva las denuncias presentadas a través de su canal interno, o no practique ante éstas ningún tipo de pesquisa o lo haga de forma deficiente (lo cual deberá tenerse en cuenta a efectos del art. 31 bis 5. 4º CP); y, otra muy distinta que, habiendo recabado una importante información al respecto, se decida no hacer nada con dicho material más allá de servir de base para la imposición de una sanción o la realización de cambios organizativos, etc.

  Así, dado que la persona jurídica goza en el proceso penal de los derechos proclamados en el art. 24.2 CE, el no denunciarse a sí misma ante las autoridades no debe ser valorado como indicio de «ineficacia» o «inoperatividad» del canal. Lo único que hay aquí es una decisión legítima y amparada por el derecho a no autoinculparse. De lo contrario, la exigencia de poner en conocimiento de las autoridades los hechos aparentemente delictivos atentaría claramente contra esta primera manifestación del derecho a no autoincriminarse (al que le siguen otras como son el derecho a no declarar contra sí mismo, a no confesarse culpable y a guardar silencio). En este sentido, una vez más, nos mostramos en contra de opiniones como la que seguidamente reproducimos: «Necesariamente se tiene que iniciar una colaboración con las autoridades competentes en el marco del proceso penal que presenta auténticas dificultades porque no existe una regulación procesal adecuada para encaminar esta colaboración»[40].

  Con todo, no debemos olvidar que en determinados ámbitos (como algunos procedimientos de comprobación o inspección) la persona jurídica puede verse conminada a «colaborar» con la Administración bajo apercibimiento de sanción u otro tipo de consecuencias.

[40] Etxeberria Bereziartua, ««Whistleblowing»…», *op. cit.*, p. 4.

5. La trasposición de la normativa europea: el Anteproyecto de Ley reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción

En las líneas que siguen, pasaremos a comentar algunos de los aspectos más importantes que presenta el Anteproyecto de Ley reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción por la que se transpone la Directiva (UE) 2019/1937 del Parlamento Europeo y del Consejo, de 23 de octubre de 2019, relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión. Para ello, nos centraremos en las principales deficiencias que alberga el citado texto, así como en las contradicciones que presenta en relación con lo dispuesto en la norma europea.

5.1. Sujetos obligados del sector privado

El artículo 10.1 impone la obligación de disponer de un «sistema interno de información» a:

a) Las personas físicas o jurídicas del sector privado que tengan contratados 50 o más trabajadores; y,

c) Los partidos políticos, los sindicatos, las patronales y las fundaciones creadas por unos y otros, siempre que reciban o gestionen fondos públicos.

Por el contrario, la letra b) de dicho precepto prevé que aquellas personas jurídicas del sector privado que entren en el ámbito de aplicación de los actos de la Unión Europea en materia de servicios, productos y mercados financieros, prevención del blanqueo de capitales o de la financiación del terrorismo, seguridad del transporte y protección del medio ambiente a que se refieren las partes I.B y II del anexo de la Directiva (UE) 2019/1937 *se regularán por su normativa específica con independencia del número de trabajadores con que cuenten*. En estos casos, la presente ley será de aplicación en lo no regulado por su normativa específica.

Considerándose incluidas en el párrafo anterior las personas jurídicas que, pese a no tener su domicilio en territorio nacional, desarrollen en España actividades a través de sucursales o agentes o mediante prestación de servicios sin establecimiento permanente.

El art. 11.1, por su parte, contempla una previsión específica para los grupos de sociedades. Así, se establece que «En el caso de un grupo de empresas conforme al artículo 42 del Código de Comercio, la sociedad dominante aprobará una política general relativa al sistema interno de

información a que se refiere el artículo 6 y la defensa del informante, y asegurará la aplicación de sus principios en todas las entidades que lo integran, sin perjuicio de la autonomía e independencia de cada sociedad, subgrupo o conjunto de sociedades integrantes que, en su caso, pueda establecer el respectivo sistema de gobierno corporativo o de gobernanza del Grupo, y de las modificaciones o adaptaciones que resulten necesarias para el cumplimiento de la normativa aplicable en cada caso».

A nuestro juicio, la previsión legal no conmina a que en estos casos se establezca un único canal de denuncias para todas las empresas que formen parte del grupo, sino que se refiere a que «la política general relativa al sistema interno de información» sea única y seguida por todas las sociedades integrantes. Ahora bien, tampoco parece haber impedimento alguno para que así sea, esto es, que pueda haber un único canal de denuncias compartido por todas ellas. Así parece desprenderse de la previsión contenido en el art. 11.2: «El Responsable del Sistema y el sistema interno de información podrá ser uno para todo el grupo, o bien uno para cada sociedad integrante del mismo, subgrupo o conjunto de sociedades, en los términos que se establezcan por la citada política».

Por otro lado, la autonomía e independencia que se reconoce a *cada sociedad, subgrupo o conjunto de sociedades integrantes* debe entenderse, en nuestra opinión, como una habilitación para ampliar, desarrollar y adecuar a la idiosincrasia de cada entidad de las que conformen el grupo dichas pautas generales (aprobadas por la matriz), pero, en ningún caso, contradecirlas.

Y, por último, el art. 12 expresa que «Las personas jurídicas del sector privado que tengan entre 50 y 249 trabajadores y que así lo decidan, podrán compartir entre sí el sistema interno de información y los recursos destinados a la gestión y tramitación de las comunicaciones, tanto si la gestión del sistema se lleva a cabo por la propia entidad como si se ha externalizado, respetándose en todo caso las garantías previstas en esta ley».

Se trata, pues, de una previsión tendente a facilitar la incorporación de dichos mecanismos ante el innegable coste económico que tiene hacerlo. Pero, en estos casos, entendemos que lo que se permite compartir es la plataforma, no que se tenga acceso a las comunicaciones de una u otra empresa de forma indiscriminada. Por ello, o el sistema se diseña de forma que, aunque existiendo un único canal funcione de forma autónoma según la empresa de la que se trate; o, lo mejor será, para evitar cualquier problema, que se externalice (como de hecho también contempla el precepto).

En cualquier caso, debemos destacar que el legislador español parece haber decidido no obligar a las entidades jurídicas del sector privado que cuenten con menos de 50 trabajadores a dotarse de dichos canales de información, aun cuando la Directiva europea sí lo permite en su art. 8.

Esta es una decisión que, en principio, debe ser criticada por nuestra parte, pues, si bien es cierto que el tejido empresarial español está formado en su mayoría por pequeñas y medianas empresas (las cuales quedarían excluidas de la citada obligación), consideramos que aquellas que contasen con 30 o más trabajadores podrían quedar sujetas a tal imperativo (más allá de que, aquí con más sentido, se les permitiese compartir tales recursos con otras empresas). Pero, a la par, también somos conscientes, precisamente, del coste que podría suponer para este tipo de empresas el hecho no ya de adoptar todo un sistema de *compliance*, sino, de tener que incorporar estos mecanismos de denuncia internas. Con todo, una vía para fomentar tales canales podría ser a través de planes específicos de las Administraciones Públicas que ayudasen a cofinanciar tal gasto.

E igualmente, la obligación para partidos o sindicatos que, *a priori*, debe ser bienvenida, nos resulta matizable, pues, el hecho de que queden obligados «siempre que reciban o gestionen fondos públicos» genera una importante distorsión: también hay partidos políticos y sindicatos de pequeñas dimensiones que no disponen de los mismos recursos para atender tal compromiso; y, sin embargo, aquí no se hace mayor distinción, cuando así debiera ser.

5.2. Materias objeto de denuncia

En cuanto al objeto de comunicación (denuncia), el art. 2.1 señala que la presente ley protege a las personas físicas que informen, a través de alguno de los procedimientos previstos en ella, de:

- Letra a):

Cualesquiera acciones u omisiones que puedan constituir infracciones del Derecho de la Unión Europea, *siempre que:*

— entren dentro del ámbito de aplicación de los actos de la Unión enumerados en el Anexo de la Directiva (UE) 2019/1937, con independencia de la calificación que de las mismas realice el ordenamiento jurídico interno.

Se trata de los siguientes: contratación pública; servicios, productos y mercados financieros, y prevención del blanqueo de capitales y la financiación del terrorismo; seguridad de los productos y conformidad; seguridad del transporte; protección del medio ambiente; protección frente a las radiaciones y seguridad nuclear; seguridad de los alimentos y los piensos, sanidad animal y bienestar de los animales; salud pública; protección de los consumidores; protección de la privacidad y de los datos personales, y seguridad de las redes y los sistemas de información.

— afecten a los intereses financieros de la Unión tal y como se contempla en el artículo 325 del TFUE; o,

— incidan en el mercado interior, tal y como se contempla en el artículo 26, apartado 2 del TFUE, incluidas las infracciones de las normas de la Unión en materia de competencia y ayudas otorgadas por los Estados, así como las infracciones relativas al mercado interior en relación con los actos que infrinjan las normas del impuesto sobre sociedades o a prácticas cuya finalidad sea obtener una ventaja fiscal que desvirtúe el objeto o la finalidad de la legislación aplicable al impuesto sobre sociedades.

• Letra b):

— Acciones u omisiones que puedan ser constitutivas de infracción penal.

— Acciones u omisiones que puedan ser constitutivas de infracción administrativa grave o muy grave.

— Cualquier vulneración del resto del ordenamiento jurídico siempre que, en cualquiera de los casos, afecten o menoscaben directamente el interés general, y no cuenten con una regulación específica. En todo caso, se entenderá afectado el interés general cuando la acción u omisión de que se trate implique quebranto económico para la Hacienda Pública.

La enumeración en términos tan genéricos como amplios efectuada por el citado precepto resulta desde nuestro punto de vista intolerable. Así pues, entendemos que, por ejemplo, en el caso de las conductas que «puedan» ser constitutivas de infracción penal, podría emplearse algún criterio que acotase tal parámetro, como:

a) en atención a su gravedad: delitos graves, menos graves o leves;

b) en atención a su naturaleza: socioeconómicos, o solo los relacionados con el ámbito de la «corrupción», etc.; o,

c) aquellos atribuibles penalmente a una persona jurídica.

No tenemos una opinión formada sobre cuál de ellos (u otros) debiera ser el criterio rector, pero, sí tenemos claro que, en todo caso, el legislador debiera emplear un parámetro algo más preciso.

Y, en cualquier caso, debemos poner de manifiesto que, recurrir a criterios como el de «acciones u omisiones que puedan ser constitutivas de infracción penal», implica una primera calificación jurídica que puede ser cuestionada y cuestionable, con los problemas que ello puede arrastrar.

Con todo, esta enumeración que hemos extraído de la letra b) no se corresponde exactamente con el tenor literal que, de forma confusa, alude a: «acciones u omisiones que puedan ser constitutivas de infracción penal o administrativa grave o muy grave o cualquier vulneración del resto del ordenamiento jurídico siempre que, en cualquiera de los casos, afecten o menoscaben directamente el interés general».

Así, por ejemplo, el CGPJ, en su Informe de 26 de mayo de 2022 (p. 28), alude a:

— infracciones penales o administrativas, graves o muy graves; y, a

— vulneraciones del ordenamiento jurídico español

Entendiendo que, en cualquier caso, deben afecten directamente al interés general.

En nuestra opinión, aunque no lo compartamos, resulta plausible entender, como hace el CGPJ, que solo podrán ser objeto de comunicación las acciones u omisiones que consistan en infracciones (penales o administrativas) graves o muy graves. Pero, lo que ya no puede asumirse es que, dentro de éstas, solo se incluyan las que afecten o menoscaben directamente «el interés general». Así las cosas, a nuestro juicio, la exigencia de afectación al interés general solo cabe predicarla respecto de «cualquier vulneración del resto del ordenamiento jurídico», pues, a pesar de lo impreciso del término, esto permite que no cualquier infracción del «resto del ordenamiento jurídico» sea denunciable (de lo contrario, todo podría ser objeto de comunicación).

Para finalizar, resta decir que, en opinión del CGPJ (Informe, p. 30), el concepto de infracción que maneja el art. 2 del Anteproyecto debería ampliarse, no pudiéndose pasar por alto que el Considerando 42 de la Directiva europea señala que «La detección y la prevención efectivas de perjuicios graves para el interés público exige que el concepto de infracción incluya también prácticas abusivas, como establece la jurisprudencia del Tribunal de Justicia, a saber, actos u omisiones que no parecen ilícitos desde el punto de vista formal, pero que desvirtúan el objeto o la finalidad de la ley».

5.3. Sujetos que gozan de protección

El art. 3, por su parte, enumera el elenco de sujetos que gozan de protección cuando informen de alguna de las cuestiones enumeradas en el art. 2. Se trata de los siguientes sujetos:

1) Informantes que trabajen en el sector privado o público y que hayan obtenido información sobre infracciones en un contexto laboral o profesional, comprendiendo en todo caso:

a) las personas que tengan la condición de empleados públicos y trabajadores por cuenta ajena;

b) los autónomos;

c) los accionistas, partícipes y personas pertenecientes al órgano de administración, dirección o supervisión de una empresa, incluidos los miembros no ejecutivos;

d) cualquier persona que trabaje para o bajo la supervisión y la dirección de contratistas, subcontratistas y proveedores.

2) Informantes que comuniquen o revelen públicamente información sobre infracciones obtenida en el marco de una relación laboral o estatutaria ya finalizada, voluntarios, becarios, trabajadores en periodos de formación con independencia de que perciban o no una remuneración, así como a aquéllos cuya relación laboral todavía no haya comenzado, en los casos en que la información sobre infracciones haya sido obtenida durante el proceso de selección o de negociación precontractual.

3) Representantes legales de las personas trabajadoras en el ejercicio de sus funciones de asesoramiento y apoyo al informante.

Por otro lado, el apartado cuarto extiende dicha protección a:

a) Personas físicas que, en el marco de la organización en la que preste servicios el informante asistan al mismo en el proceso.

b) Personas físicas que estén relacionadas con el informante y que puedan sufrir represalias, como compañeros de trabajo o familiares del informante, y

c) Personas jurídicas, para las que trabaje o con las que mantenga cualquier otro tipo de relación en un contexto laboral o en las que ostente una participación significativa. A estos efectos, se entiende que la participación en el capital o en los derechos de voto correspondientes a acciones o participaciones es significativa cuando, por su proporción, permite a la persona que la posea tener capacidad de influencia en la persona jurídica participada.

5.4. Medidas de protección y de apoyo

5.4.1. Requisitos para la concesión de protección

El art. 35.1 del Anteproyecto contempla que las personas que comuniquen o revelen infracciones (de las previstas en el art. 2) tengan derecho a protección solo cuando se cumplan las siguientes condiciones (de forma cumulativa):

a) Tengan motivos razonables para pensar que la información referida es veraz en el momento de la comunicación o revelación, aun cuando no aporten pruebas concluyentes, y que la citada información entra dentro del ámbito de aplicación de la presente ley; y

b) La comunicación o revelación se haya realizado conforme a los requerimientos previstos en esta ley.

En cuanto al primer requisito, se habla de que el denunciante tenga «motivos razonables para pensar que la información referida es veraz», aun cuando no se aporten «pruebas concluyentes». Dicha cláusula, a nuestro juicio, debe entenderse como un requisito de admisibilidad de la denuncia basado en una aportación mínima de evidencias que sustenten la versión de los hechos que se han puesto en conocimiento. La veracidad exige que se trate de información contrastada (verificada). Es decir, que, sin llegar a ser incontestable (concluyente) tenga un mínimo rigor. Con todo, debemos ser conscientes de que el informante no siempre tendrá acceso al material (documentos, información, datos) que de sustento a su denuncia. Incluso puede que el apoderamiento de dicho contenido pudiera ser delictivo. Por ello, en la práctica puede que el estándar de «veracidad» acabe traduciéndose en que se trate de un relato creíble o «razonable» y que la denuncia sea admitida sin perjuicio de las posteriores comprobaciones que pudieran hacerse (las cuales podrían desencadenar en un «archivo» de la misma».

Ahora bien, debe insistirse en que, aquí, este precepto en puridad regula las condiciones que deben darse para otorgar protección al denunciante. Pero, a nuestro parecer, como dijimos, esta previsión debe conectarse con su reverso: la admisibilidad de la denuncia y, con ella, la concesión de la protección. Así, por ejemplo, para el caso concreto de las denuncias formuladas ante la Autoridad Independiente de Protección del Informante, el art. 18.2 a) estima como causas de inadmisión: que los hechos carezcan de toda verosimilitud; o, que carezca manifiestamente de fundamento o existan indicios racionales de haberse obtenido de forma ilícita. No sucede lo mismo con las denuncias emitidas ante canales internos. De ahí que deba extenderse a éstos lo dicho más arriba.

Por otro lado, la segunda condición atiende a cuestiones más bien formales o procedimentales.

Por el contrario, el apartado segundo del art. 31 excluye expresamente de la protección prevista en esta ley a aquellas personas que comuniquen o revelen:

a) Informaciones contenidas en comunicaciones que hayan sido inadmitidas por alguna de las causas previstas en el artículo 18.2 a).

b) Informaciones vinculadas a reclamaciones sobre conflictos interpersonales o que afecten únicamente al informante y a las personas a las que se refiera la comunicación o revelación.

c) Informaciones que ya estén completamente disponibles para el público, o que constituyan meros rumores;

d) Informaciones que se refieran a acciones u omisiones no comprendidas en el artículo 2.

Una vez más, a nuestro parecer, el precepto no solo enumera una lista de supuestos en los que no cabe conceder tal protección al informante, sino que debe leerse también en clave de causas de inadmisión. Así, a las ya citadas anteriormente del art. 18.2 a), deben sumarse las informaciones vinculadas a reclamaciones sobre conflictos interpersonales, las que ya estén completamente disponibles para el público, y aquellas que constituyan meros rumores. Y, naturalmente, como reza el precepto, aquellas que queden fuera del ámbito material de la ley.

El apartado tercero, por su parte, contempla una cláusula que debe ser destacada, pues, si, como resulta evidente, no puede brindarse protección a quien no se ha identificado (anonimato), esta situación es reversible. Y, por ello, se establece que «Las personas que hayan comunicado o revelado públicamente información sobre acciones u omisiones a que se refiere el artículo 2 de forma anónima pero que posteriormente hayan sido identificadas y cumplan las condiciones previstas en esta ley, tendrán derecho a la protección que la misma contiene».

En último lugar, el apartado cuarto prevé otorgar protección incluso cuando las personas no informen a través de los canales diseñados por esta ley, sino que lo hagan ante las instituciones, órganos u organismos pertinentes de la Unión Europea cuando se trate de infracciones que entren en el ámbito de aplicación de la Directiva (UE) 2019/1937, señalándose que, en tales casos, «tendrán derecho a protección con arreglo a lo dispuesto en la presente ley en las mismas condiciones que una persona que haya informado por canales externos».

5.4.2. Prohibición de represalias: listado

En realidad, las auténticas medidas de protección son las enunciadas en el art. 36 del Anteproyecto. Este precepto proclama en su apartado primero la prohibición expresa de actos constitutivos de represalia, incluidas las amenazas de represalia y las tentativas de represalia contra las personas que presenten una comunicación conforme a lo previsto en la presente ley.

El apartado segundo recoge qué se entiende por represalia: cualesquiera actos u omisiones que estén prohibidos por la ley, o que, de forma directa o indirecta, supongan un trato desfavorable que sitúe a las personas que las sufren en desventaja particular con respecto a otra en el contexto laboral o profesional, sólo por su condición de informantes, o por haber realizado una revelación pública, y siempre que tales actos u

omisiones se produzcan mientras dure el procedimiento de investigación o en los dos años siguientes a la finalización del mismo o de la fecha en que tuvo lugar la revelación pública. Exceptuándose el supuesto en que dicha acción u omisión pueda justificarse objetivamente en atención a una finalidad legítima y que los medios para alcanzar dicha finalidad sean necesarios y adecuados. Como señala el CGPJ, en su Informe de 26 de mayo de 2022 (p. 72), el prelegislador introduce en la definición de las acciones u omisiones que pueden categorizarse como represalias una acotación temporal en cuya virtud solo se reputaran tales aquellas que se produzcan «mientras dure el procedimiento de investigación o en los dos años siguientes a la finalización del mismo o de la fecha en que tuvo lugar la revelación pública». Pero, el art. 5 de la Directiva define la represalia como «toda acción u omisión, directa o indirecta, que tenga lugar en un contexto laboral, que esté motivada por una denuncia interna o externa o por una revelación pública y que cause o pueda causar perjuicios injustificados al denunciante». Así, «la definición propuesta por el prelegislador introduce, por tanto, una limitación temporal que restringe o acota de manera relevante el número de acciones u omisiones que pueden catalogarse como represalias a los efectos de la aplicación de la norma sin que la Directiva objeto de trasposición avale tal limitación o restricción».

Por último, el apartado tercero recoge, a título enunciativo (*numerus apertus*), la clase de represalias frente al alertador que quedan terminantemente prohibidas:

a) Suspensión del contrato de trabajo, despido o extinción de la relación laboral o estatutaria, incluyendo la terminación anticipada de un contrato de trabajo temporal una vez superado el período de prueba, o terminación anticipada o anulación de contratos de bienes o servicios, imposición de cualquier medida disciplinaria, degradación o denegación de ascensos y cualquier otra modificación sustancial de las condiciones de trabajo, salvo que estas medidas se llevaran a cabo dentro del ejercicio regular del poder de dirección al amparo de la legislación laboral o reguladora del estatuto del empleado público correspondiente, por circunstancias, hechos o infracciones acreditadas, y ajenas a la presentación de la comunicación.

b) Daños, incluidos los de carácter reputacional, o pérdidas económicas, coacciones, intimidaciones, acoso u ostracismo.

c) Evaluación o referencias negativas respecto al desempeño laboral o profesional.

d) Inclusión en listas negras o difusión de información en un determinado ámbito sectorial, que dificulten o impidan el acceso al empleo o la contratación de obras o servicios.

e) Anulación de una licencia o permiso.

Llegados a este punto, es de resaltar que el legislador español no ha previsto otra serie de represalias a las que sí se alude en el art. 19 de la Directiva europea. Se trata concretamente de las siguientes: 1) denegación de formación; 2) discriminación, o trato desfavorable o injusto; 3) no conversión de un contrato de trabajo temporal en uno indefinido, en caso de que el trabajador tuviera expectativas legítimas de que se le ofrecería un trabajo indefinido; y, 4) referencias médicas o psiquiátricas.

En otro orden de cosas, el apartado cuarto prevé que la persona que viera lesionados sus derechos por causa de su comunicación o revelación una vez transcurrido el plazo de un año a que se refiere este artículo pueda solicitar la protección de la autoridad competente que, excepcionalmente y de forma justificada, podrá extender el periodo de protección, previa audiencia de las personas u órganos que pudieran verse afectados. Esta previsión contradice el plazo estipulado en «este artículo», que no es de un año, sino de dos, como prevé el apartado segundo. Con todo, esta previsión no debe entenderse como un periodo de carencia durante el cual el denunciante no puede solicitar amparo; sino, que alude al tiempo durante el cual se extiende la protección. Por tanto, lo que permite el apartado cuarto es una ampliación del plazo original (dos años).

Por último, advertir que, en el ámbito penal, la protección del «denunciante» puede conferirse a través de tipos delictivos como los que a continuación mencionaremos:

1) amenazas: constitutivas de delito (art. 169 CP); o, no constitutivas de delito (art. 171 CP);
2) coacciones (arts. 172.1 y 3 CP);
3) acoso laboral (art. 173.1 CP);
4) art. 464 CP: intentar influir con violencia o intimidación sobre el denunciante para que modifique su actuación procesal (apdo. 1º); y, realizar cualquier acto atentatorio contra la vida, integridad, libertad, libertad sexual o bienes, como represalia contra las personas citadas en el apartado anterior, por su actuación en procedimiento judicial (apdo. 2º).

5.4.3. Exclusión de la responsabilidad en que se hubiere podido incurrir a raíz de la denuncia

El art. 38.1 del Anteproyecto contempla otra modalidad de «protección» del informante, pero, esta vez, lo hace excluyendo la posibilidad de perseguir (responsabilizar) al denunciante por determinadas comunicaciones. Así, de forma genérica se establece que:

> «No se considerará que las personas que comuniquen información sobre las acciones u omisiones recogidas en esta ley o que hagan una revelación pública de conformidad con la presente ley hayan infringido ninguna restricción de revelación de información, y éstas no incurrirán en responsabilidad de ningún tipo en relación con dicha comunicación o revelación pública, siempre que tuvieran motivos razonables para pensar que la comunicación o revelación pública de dicha información era necesaria para revelar una acción u omisión en virtud de la presente ley, todo ello sin perjuicio de lo dispuesto en el artículo 2.3. Esta medida no afectará a las responsabilidades de carácter penal.
>
> Lo previsto en el párrafo anterior se extiende a la comunicación de informaciones realizadas por los representantes de las personas trabajadoras, aunque se encuentren sometidas a obligaciones legales de sigilo o de no revelar información reservada. Todo ello sin perjuicio de las normas específicas de protección aplicables conforme a la normativa laboral».

Es importante destacar, a este respecto, que, en ningún caso, se excluye de responsabilidad a quien efectúe una comunicación que pueda constituir un delito de revelación de secretos (art. 197.3 CP). El texto lo deja claro cuando alude a que «*Esta medida no afectará a las responsabilidades de carácter penal*». Más allá de que, luego, en algún supuesto concreto, pueda alegarse la concurrencia de alguna circunstancia eximente. En este sentido, podría aducirse que la puesta en conocimiento de determinada información (lejos de reputarse delictiva) suponía bien estar obrando en cumplimiento de un deber o en el ejercicio legítimo de un derecho, como es el de denunciar comportamientos aparentemente delictivos o (cuanto menos) irregulares (art. 20.7º CP); o, bien, plantear un estado de necesidad (art. 20.5º CP) justificante o excusante según si el bien jurídico que se estuviera poniendo en valor fuere de mayor o igual entidad que el que se sacrifica (el secreto de las comunicaciones, intimidad, etc.) Piénsese, por ejemplo, que a raíz de la denuncia se hubiere destapado una gran trama de corrupción política/urbanística o un gran fraude a consumidores; o, que se hubiere apreciado una insolvencia punible. Posiblemente, en el primer caso el estado de necesidad podría ser justificante y, en el segundo, excusante. Con todo, convendría recordar que aquí estamos refiriéndonos a la posible exención de responsabilidad penal por quedar amparada la conducta reveladora en alguna causa de las previstas en el art. 20 CP. Pero, esto es una cosa y, otra muy distinta, que las pruebas aportadas de este modo fueren válidas para sustentar una condena por el delito que se hubiere denunciado. A este respecto, en cuanto a la aportación de pruebas obtenidas mediante vulneración de derechos fundamentales por un particular convendría tener presente la doctrina sentada por el Tribunal Supremo en la STS 116/2017, de 23 de febrero (caso Falciani) y ratificada por el Tribunal Constitucional (STC 97/2019, de 16 de julio), pues, no todas estas actuaciones acaban violando lo dispuesto en el art. 11 LOPJ[41].

[41] *Vid*., para más detalle, León Alapont, «Retos jurídicos..», *op. cit*., p. 21 y ss.

En línea con lo anterior, el apartado segundo establece que «Los informantes no incurrirán en responsabilidad respecto de la adquisición o el acceso a la información que es comunicada o revelada públicamente, siempre que dicha adquisición o acceso no constituya un delito». Aquí ya no se trataría, como sucedía en el otro caso, de revelar de forma ilícita una información; sino, de obtener o acceder a ella incurriendo en delito (arts. 197. 1 y 2 CP).

El apartado tercero anuda la exclusión de responsabilidad del informante a que la comunicación verse sobre las acciones u omisiones recogidas en esta ley o que hagan una revelación pública de conformidad con la presente ley. Por ello se advierte de que: «Cualquier otra posible responsabilidad de los informantes derivada de actos u omisiones que no estén relacionados con la comunicación o la revelación pública o que no sean necesarios para revelar una infracción en virtud de la presente ley serán exigibles conforme a la normativa aplicable».

Por último, los apartados cuarto y quinto contemplan unas previsiones específicas para determinados procedimientos:

> «4. En los procedimientos laborales ante un órgano jurisdiccional relativos a los perjuicios sufridos por los informantes, una vez que el informante haya demostrado razonablemente que ha comunicado o ha hecho una revelación pública de conformidad con la presente ley y que ha sufrido un perjuicio, se presumirá que el perjuicio se produjo como represalia por informar o por hacer una revelación pública. En tales casos, corresponderá a la persona que haya tomado la medida perjudicial probar que esa medida se basó en motivos debidamente justificados no vinculadas a la comunicación o revelación pública».
>
> «5. En los procesos judiciales civiles o laborales, incluidos los relativos a difamación, violación de derechos de autor, vulneración de secreto, infracción de las normas de protección de datos, revelación de secretos empresariales, o a solicitudes de indemnización basadas en el derecho laboral o estatutario, las personas a que se refiere la presente ley no incurrirán en responsabilidad de ningún tipo como consecuencia de comunicaciones o de revelaciones públicas protegidas por la misma. Dichas personas tendrán derecho a alegar en su descargo el haber comunicado o haber hecho una revelación pública, siempre que tuvieran motivos razonables para pensar que la comunicación o revelación pública era necesaria para poner de manifiesto una infracción en virtud de la presente ley».

5.4.4. Los denominados «programas de clemencia»: repercusión en el ámbito administrativo

El art. 40.1 del Anteproyecto prevé que cuando una persona que hubiera participado en la comisión de la infracción administrativa objeto de la información sea la que informe de la existencia de la misma mediante la presentación de la información y siempre que la misma hubiera sido presentada con anterioridad a que hubiera sido notificada la

incoación del procedimiento de investigación o sancionador, el órgano competente para resolver el procedimiento, mediante resolución motivada, podrá eximirle del cumplimiento de la sanción administrativa que le correspondiera siempre que resulten acreditados en el expediente los siguientes extremos:

a) Haber cesado en la comisión de la infracción en el momento de presentación de la comunicación o revelación e identificado, en su caso, al resto de las personas que hayan participado o favorecido aquella.

b) Haber cooperado plena, continua y diligentemente a lo largo de todo el procedimiento de investigación.

c) Haber facilitado información veraz y relevante, medios de prueba o datos significativos para la acreditación de los hechos investigados, sin que haya procedido a la destrucción de estos o a su ocultación, ni haya revelado a terceros, directa o indirectamente a terceros su contenido.

d) Haber procedido a la reparación del daño causado que le sea imputable.

Se trata, como puede observarse de una medida discrecional («podrá»), debiéndose reunir todos y cada uno de los cuatro requisitos (por ser acumulativos). En relación con esto último, el apartado segundo contempla que cuando estos requisitos solo se cumplan parcialmente, incluida la reparación parcial del daño, quedará a criterio de la autoridad competente, previa valoración del grado de contribución a la resolución del expediente, la posibilidad de atenuar la sanción que habría correspondido a la infracción cometida, siempre que el informante o autor de la revelación no haya sido sancionado anteriormente por hechos de la misma naturaleza que dieron origen al inicio del procedimiento.

Por su parte, el apartado tercero prevé que la atenuación de la sanción pueda extenderse al resto de los participantes en la comisión de la infracción, en función del grado de colaboración activa en el esclarecimiento de los hechos, identificación de otros participantes y reparación o minoración del daño causado, apreciado por el órgano encargado de la resolución.

Por último, el apartado cuarto establece una excepción: «Lo dispuesto en este artículo no será de aplicación a las sanciones que pudieran imponerse por la realización de las conductas prohibidas por la Ley 15/2007, de 3 de julio, de Defensa de la Competencia. Dichas sanciones se regirán, en su caso, por lo dispuesto en los artículos 65 y 66 de la misma».

5.4.5. Medidas de apoyo

Además, el art. 37.1 del Anteproyecto prevé una serie de «medidas de apoyo» que son las siguientes:

a) Información y asesoramiento integral, accesible y gratuito, sobre los procedimientos y recursos disponibles, para la protección frente a represalias y sobre los derechos del informante.

b) Asistencia efectiva en su protección frente a represalias.

c) Apoyo financiero y psicológico, de forma excepcional, si procede tras la valoración por la Autoridad independiente de Protección del Informante de las circunstancias derivadas de la presentación de la comunicación.

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

Estas medidas de apoyo pueden ser proporcionadas tanto por la Autoridad Independiente de Protección del Informante como por los órganos competentes de las Comunidades Autónomas, según los casos (art. 41).

A nuestro juicio, lo más llamativo (y a la vez sorprendente) de este Anteproyecto es que no crea unos mecanismos específicos de auténtica reacción (protección) una vez materializadas las «represalias». Esto es, no se concreta qué sucede cuando se despide a un trabajador porque ha denunciado determinados hechos; ni cuando por igual motivo se remueve a un administrador de una empresa de su puesto; ni cuando se cercenan determinados derechos de los accionistas, etc. Y es que para encontrar las soluciones jurídicas a tales escenarios debemos acudir a mecanismos que nuestro ordenamiento jurídico ya dispone (en materia laboral, mercantil, etc.). Sin olvidar, por ejemplo, la protección que se puede dispensar en el proceso penal al testigo o a quien actúa como confidente de la policía[42]. De igual modo, cuesta pensar cómo se puede brindar protección a una persona jurídica (que también puede ser considerada susceptible de protección), de ahí que, por ejemplo, ante una anulación de una licencia pueda iniciarse un procedimiento penal por prevaricación; o, ante una campaña de desprestigio, pueden iniciarse acciones ante organismos de defensa de la competencia, etc.

Queremos con ello decir que, en este punto, tanto la Directiva como el Anteproyecto lo que hacen más bien es reforzar un mensaje: que el denunciante no está solo. Pero, nada más. Por eso se recurre a enunciar medidas como: a) ofrecer información y asesoramiento integral, accesible y gratuito, sobre los procedimientos y recursos disponibles, para la protección frente a represalias y sobre los derechos del informante; o,

[42] *Vid*., sobre estos temas, Ortiz Pradillo, J. C.: *Los delatores en el proceso penal. Recompensas, anonimato, protección y otras medidas para incentivar una colaboración eficaz con la justicia*, Madrid, Wolters Kluwer-La Ley, 2018.

asistencia efectiva en su protección frente a represalias. La novedad es que el denunciante contará, a partir de ahora, con un apoyo institucional (Autoridad Independiente y organismos autonómicos) a través del cual poder canalizar, al margen de otras vías, dicha solicitud de amparo.

5.5. Los «Sistemas internos de información»: disposiciones generales

Los arts. 5 a 9 del Anteproyecto contemplan una serie de disposiciones comunes a todos los «sistemas internos de información».

5.5.1. Sujetos u órganos responsables de su implantación y gestión

El art. 5.1 del Anteproyecto establece que el órgano de administración u órgano de gobierno de cada entidad u organismo obligado por la presente ley será el responsable de la implantación del sistema interno de información, previa consulta con la representación legal de las personas trabajadoras.

Siendo el órgano de administración u órgano de gobierno de cada entidad u organismo obligado por la presente ley será el competente para la designación de la persona física responsable de la gestión de dicho sistema («Responsable del Sistema») y de su destitución o cese (art. 9.1). Por tanto, tiene que nombrarse a un «responsable» que se encargue de la gestión de todo el sistema de información (que no solo del canal de denuncias, como veremos). A este respecto, el art. 8.1 alude a que «El procedimiento de gestión de comunicaciones será aprobado por el Responsable del Sistema, que responderá de su tramitación diligente».

El Anteproyecto permite que el «Responsable del sistema» sea un órgano colegiado. En este sentido, el art. 9.2 prevé que «Si se optase por que el Responsable del Sistema fuese un órgano colegiado, éste deberá delegar en uno de sus miembros las facultades de gestión del sistema interno de información y de tramitación de expedientes de investigación».

Por su parte, el art. 9.2 prevé, para el caso de los grupos de sociedades, que «El Responsable del Sistema y el sistema interno de información podrá ser uno para todo el grupo, o bien uno para cada sociedad integrante del mismo, subgrupo o conjunto de sociedades, en los términos que se establezcan por la citada política».

En cualquier caso, como recoge el art. 9.3 del Anteproyecto, tanto el nombramiento como el cese de la persona física individualmente designada, así como de las integrantes del órgano colegiado deberá ser notificado a la Autoridad Independiente de Protección del Informante

regulada en el título VIII en el plazo de los diez días hábiles siguientes, especificando, en el caso de su cese, las razones que han justificado el mismo.

En cuanto a este Responsable, el apartado cuarto del art. 9 contempla que «deberá desarrollar sus funciones de forma independiente y autónoma respecto del resto de los órganos de organización de la entidad u organismo». La independencia resulta difícil de predicar de un cargo que requiere ser designado (puesto por) o destituido, por lo que entendemos que, sobre todo, la nota que debe caracterizar toda su actuación es la de autonomía (respecto del resto de los órganos de organización de la entidad u organismo).

Más concretamente, el apartado quinto del art. 9 señala que, en el caso del sector privado, el Responsable del Sistema (persona física o la persona en quien el órgano colegiado responsable haya delegado sus funciones), *será un alto directivo de la entidad, que asumirá exclusivamente dichas funciones* y que ejercerá su cargo con independencia del órgano de administración o de gobierno de la misma. Por tanto, habrá incompatibilidad absoluta con el ejercicio de cualquier otro cometido dentro de la entidad. Ahora bien, sigue diciendo la disposición citada, que, cuando la naturaleza o la dimensión de las actividades de la entidad no justifiquen o permitan la existencia de un directivo Responsable del Sistema, *será posible el desempeño ordinario de las funciones del puesto o cargo con las de Responsable del Sistema, tratando en todo caso de evitar posibles situaciones de conflicto de interés*.

En último lugar, el art. 6 dispone que en las entidades u organismos en las que ya existiera un responsable de la función de cumplimiento normativo, cualquiera que fuese su denominación, podrá ser éste la persona designada como Responsable del Sistema, siempre que cumpla los requisitos establecidos en la presente ley. A este respecto, cabría apuntar que caben dos escenarios posibles:

1) aquel en que la persona jurídica decide que existe un órgano de cumplimiento (*compliance officer*) que vele por la supervisión y control del programa; y, un responsable específico solo del sistema de información interno; y,

2) aquel en que la persona jurídica decide que ambas funciones recaigan en la misma persona (u órgano).

5.5.2. Diseño de los sistemas internos de información

Como se verá, un sistema de información abarca, además del propio canal de denuncias, otros muchos aspectos. Por tanto, se trata de una política corporativa de mayor alcance (aunque, naturalmente, uno de los pilares fundamentales sea dicho canal).

En este sentido, el art. 5.2 del Anteproyecto se refiere a que los sistemas internos de información, en cualquiera de sus fórmulas de gestión, deberán:

a) Permitir comunicar información sobre las infracciones previstas en el artículo 2 a todas las personas referidas en el artículo 3.

b) Estar diseñados, establecidos y gestionados de una forma segura, de modo que se garantice la confidencialidad de la identidad del informante y de cualquier tercero mencionado en la comunicación y de las actuaciones que se desarrollen en la gestión y tramitación de la misma, la protección de datos, impidiendo el acceso de personal no autorizado.

c) Permitir la presentación de comunicaciones por escrito o verbalmente, o de ambos modos.

d) Integrar los distintos canales internos de comunicación que pudieran establecerse dentro de la entidad.

El art. 7.1 reza, en sentido similar, así: «Todos los canales internos de información de que disponga una entidad para posibilitar la presentación de información respecto de las infracciones previstas en el artículo 2 estarán integrados dentro del sistema interno de información a que se refiere el artículo 6».

e) Garantizar que las comunicaciones presentadas puedan tratarse de manera efectiva dentro de la correspondiente entidad u organismo con el objetivo de que el primero en conocer la posible irregularidad sea el propio empleador.

f) Ser independientes y aparecer diferenciados respecto de los sistemas internos de información de otras entidades u organismos, sin perjuicio de lo establecido en los artículos 12 y 13 siguientes.

g) Contar con un responsable del Sistema en los términos previstos en el artículo 10 de esta ley.

h) Contar con una política o estrategia que enuncie los principios generales en materia de sistemas internos de información y defensa del informante y que sea debidamente publicitada en el seno de la entidad u organismo.

i) Contar con un procedimiento de gestión de las comunicaciones recibidas.

j) Establecer las garantías para la protección de los informantes en el ámbito de la propia entidad u organismo, respetando, en todo caso, lo dispuesto en el artículo 9.

5.5.3. La externalización de la gestión del sistema

El art. 6.1 del Anteproyecto prevé que la gestión de los sistemas internos de información pueda llevarse a cabo dentro de la propia entidad u organismo o acudiendo a un tercero externo, en los términos previstos en esta ley (a estos efectos, según reza el precepto, se considera gestión del sistema la recepción de informaciones). Se trata, sin duda, de una opción muy recomendable, sobre todo, para personas jurídicas de gran tamaño.

Con todo, la externalización se condiciona a la concurrencia de una serie de requisitos mínimos. Así, se exige que el tercero externo ofrezca, en todo caso, garantías adecuadas de respeto de la independencia, la confidencialidad, la protección de datos y el secreto (art. 6.2). Y, en línea con lo anterior, el apartado tercero de dicho artículo establece que «La gestión del sistema interno de información por un tercero no podrá suponer un menoscabo de las garantías y requisitos que para dicho sistema establece la presente ley ni una atribución de la responsabilidad sobre el mismo en persona distinta del Responsable del Sistema».

Asimismo, el art. 6.4 prevé que el tercero externo que gestione el canal tendrá la consideración de encargado del tratamiento a efectos de la legislación sobre protección de datos personales.

5.5.4. Tipos de canales internos de información

El art. 7.2 del Anteproyecto dispone que los canales internos deberán permitir realizar comunicaciones por escrito o verbalmente, o de las dos formas.

La información se podrá realizar bien por escrito, a través de correo postal o a través de cualquier medio electrónico habilitado al efecto, o verbalmente, por vía telefónica o a través de sistema de mensajería de voz.

A solicitud del informante, también podrá presentarse mediante una reunión presencial. En estos últimos casos, bien sea realice la comunicación verbalmente bien de manera presencial, se advertirá al informante de que la comunicación será grabada y se le informará del tratamiento de sus datos de acuerdo a lo que establecen el Reglamento (UE) 2016/679 y la Ley Orgánica 3/2018, de 5 de diciembre de Protección de Datos Personales y garantía de los derechos digitales.

Al hacer la comunicación, el informante podrá indicar un domicilio, correo electrónico o lugar seguro a efectos de recibir las notificaciones.

Las comunicaciones verbales deberán documentarse de alguna de las maneras siguientes:

a) mediante una grabación de la conversación en un formato seguro, duradero y accesible; o,

b) a través de una transcripción completa y exacta de la conversación realizada por el personal responsable de tratarla.

Sin perjuicio de los derechos que le corresponden de acuerdo a la normativa sobre protección de datos, se ofrecerá al informante la oportunidad de comprobar, rectificar y aceptar mediante su firma la transcripción del mensaje.

Por otro lado, el apartado tercero conmina a que los canales internos deberán permitir la presentación y posterior tramitación de comunicaciones anónimas. Si bien, este sistema convive con el de confidencialidad (art. 5.2.b).

A este respecto, el CGPJ, en su Informe de 26 de mayo de 2022, si bien asume la posibilidad de que puedan presentarse denuncias anónimas, considera que «la identificación del informante puede coadyuvar a evitar el abuso y el uso indiscriminado de los canales de denuncias y permitir, asimismo, la efectiva protección de los whistleblowers contra posibles represalias, además, de permitir que sea posible recabar más información sobre los hechos denunciados que pueda ser relevante para la resolución del conflicto, y ello en línea con los sostenido por el Supervisor Europeo de Protección de datos personales en la Guía de procedimiento referida» (p. 63).

Por último, el apartado cuarto establece que los canales internos de comunicación podrán estar habilitados por la entidad que los gestione para la recepción de cualesquiera otras comunicaciones o informaciones fuera del ámbito establecido en el artículo 2, si bien dichas comunicaciones y sus remitentes quedarán fuera del ámbito de protección dispensado por la misma. Esta es una muestra más de las múltiples utilidades o funciones que un canal interno puede tener (más allá de la denuncia de «infracciones»).

5.5.5. El procedimiento de gestión de las comunicaciones recibidas

El art. 8.1 regula que el procedimiento de gestión de comunicaciones sea aprobado por el Responsable del Sistema, que responderá de su tramitación diligente.

En este sentido, a diferencia de lo que sucede en el caso de la Autoridad Independiente de Protección del Informante (arts. 17 y ss.), el Anteproyecto no alberga ninguna disposición procedimental al respecto, dejando tal cuestión al albur de las previsiones que dicte el «Responsable del Sistema» (de la entidad privada). Esta circunstancia, a nuestro juicio, resulta incomprensible, pues, ¡para eso están las leyes!: para armonizar o unificar criterios en pro de una «mínima» seguridad jurídica (que aquí brilla por su ausencia).

Este déficit, que principalmente afectará a la fase de admisión de las comunicaciones (primera criba), puede acabar conduciendo a que los canales externos como los de la Autoridad Independiente y los de los órganos autonómicos homónimos (sobre todo estos últimos) se vean saturados. Acudiendo a ellos tras la insatisfactoria respuesta ofrecida por unos canales internos sin criterios claros o ampliamente discrecionales.

Por otro lado, el art. 8.2 del Anteproyecto alude a la necesidad de establecer un procedimiento que establezca las previsiones necesarias para que el sistema interno de información y los canales internos existentes cumplan con los requisitos establecidos en la presente ley. En particular, el procedimiento responderá al siguiente contenido mínimo y principios:

a) Identificación del canal o canales internos a los que se asocian;

b) Establecimiento de la necesidad de enviar acuse de recibo de la comunicación al informante, en el caso de que este se identifique, en el plazo de siete días naturales siguientes a su recepción, salvo que ello pueda poner en peligro la confidencialidad de la comunicación;

c) Previsión de la posibilidad de mantener la comunicación con el informante y, si se considera necesario, de solicitar a la persona informante información adicional;

d) Establecimiento del derecho del informante a que se le informe de las acciones u omisiones que se le atribuyen, y a ser oído en cualquier momento. Dicha comunicación tendrá lugar en el tiempo y forma que se considere adecuado para garantizar el buen fin de la investigación;

e) Exigencia del respeto a la presunción de inocencia, el derecho a ser oído y el honor de las personas investigadas;

f) Determinación de la duración máxima de las actuaciones de investigación, que no podrá ser superior a tres meses a contar desde la recepción de la comunicación, salvo casos de especial complejidad que requieran una ampliación del plazo, en cuyo caso, este podrá extenderse hasta un máximo de otros tres meses adicionales;

g) Inclusión de información clara y fácilmente accesible sobre los canales externos de comunicación ante las autoridades competentes y, en su caso, ante las instituciones, órganos u organismos de la Unión Europea;

h) Garantía de la confidencialidad cuando la comunicación sea remitida a personal no competente y, en estos supuestos, establecimiento de la obligación del receptor de la comunicación de remitirla inmediatamente al Responsable del Sistema;

i) Respeto de las disposiciones sobre protección de datos personales de acuerdo a lo previsto en el título VI.

Hemos de destacar el contenido de la letra b) porque, a juicio del CGPJ (Informe, p. 40), la excepción que contempla dicho precepto para no enviar acuse de recibo al informante debiera suprimirse. Argumenta este órgano, en el Informe de 26 de mayo de 2022, que «aunque la norma europea prevé en el apartado f) del mismo artículo 9 la posibilidad de que no se haya emitido un acuse de recibo, ello parece responder a una simple salvaguarda para la fijación de los plazos de tramitación en caso de un error o mala praxis en la emisión del acuse de recibo, resultando este, y su plazo, preceptivo».

También debemos resaltar la previsión albergada en la letra f) del art. 8.2 porque en ella se dice que la duración máxima de las actuaciones de investigación no podrá ser superior a tres meses a contar desde la recepción de la comunicación, salvo casos de especial complejidad que requieran una ampliación del plazo, en cuyo caso, éste podrá extenderse hasta un máximo de seis meses. En este sentido, queremos manifestar que la regla general es que las investigaciones no se prolonguen durante más de 3 meses, lo cual nos parece una pretensión bienintencionada, pero, puede que poco real. Incluso, la excepción de los 6 meses (la norma no define qué casos deben tenerse por «complejos») puede resultar insuficiente. Con todo, si echamos un vistazo a la Directiva europea, el art. 9.1.f) únicamente habla de una duración máxima de 3 meses (por lo que el legislador español parece haber sido más generoso). De hecho, el CGPJ, en su Informe de 26 de mayo de 2022, aboga por contemplar un único plazo de 3 meses en consonancia con la norma europea. A nuestro juicio, dicha recomendación no debería ser admitida.

5.6. Disposiciones comunes a los canales internos

Los arts. 25 y 26 del Anteproyecto regulan una serie de disposiciones comunes a los canales internos tanto de las entidades privadas como públicas.

En primer lugar, el art. 25 se ocupa de velar por un aspecto que consideramos esencial en todo sistema de gestión de denuncias. Se trata de poner en conocimiento de los potenciales usuarios la información necesaria para que tales canales sean utilizados y quien pretenda hacerlo sepa qué, cómo, cuándo y dónde puede denunciar. En este sentido, refiriéndose a los canales internos, se establece que «Los sujetos comprendidos dentro del ámbito de aplicación de la presente ley proporcionarán la información adecuada de forma clara y fácilmente accesible, sobre el uso de los canales internos de información que hayan implantado, así como sobre los principios esenciales del procedimiento de gestión. En caso de contar con una página web, dicha información deberá constar en la página de inicio, en una sección separada y fácilmente identificable». Asimismo, el art. 32.5 alude a esta misma cuestión cuando se refiere a que los

empleados y terceros deberán estar informados acerca de la existencia de los sistemas de información.

Y, ya con referencias a la Autoridad Independiente (u organismos autonómicos equivalentes), el art. 25 se refiere a que, de igual modo, publicarán, en una sección separada, fácilmente identificable y accesible de su sede electrónica, como mínimo, la información siguiente:

a) Las condiciones para poder acogerse a la protección en virtud de la presente ley;

b) Los datos de contacto para los canales externos de información previstos en el título III, en particular, las direcciones electrónica y postal y los números de teléfono asociados a dichos canales, indicando si se graban las conversaciones telefónicas;

c) Los procedimientos de gestión, incluida la manera en que la autoridad competente puede solicitar al informante aclaraciones sobre la información comunicada o que proporcione información adicional, el plazo para dar respuesta al informante, en su caso, y el tipo y contenido de dicha respuesta;

d) El régimen de confidencialidad aplicable a las comunicaciones, y en particular, la información sobre el tratamiento de los datos personales de conformidad con lo dispuesto en el Reglamento (UE) 2016/679, la Ley Orgánica 3/2018, y el título VI.

e) Las vías de recurso y los procedimientos para la protección frente a represalias, y la disponibilidad de asesoramiento confidencial. En particular, se contemplarán las condiciones de exención de responsabilidad y los programas de clemencia a los que se refieren los artículos 40 y 41.

f) Los datos de contacto de la Autoridad Independiente de Protección del Informante prevista en el título VIII o de la autoridad u organismo competente de que se trate.

En segundo lugar, el art. 26 se ocupa de regular el registro de comunicaciones. A este respecto, se señala que todos los sujetos obligados, de acuerdo con lo dispuesto en esta ley, a disponer de un canal interno de informaciones, con independencia de que formen parte del sector público o del sector privado, deberán contar con un libro-registro de las comunicaciones recibidas y de las investigaciones internas a que hayan dado lugar, garantizando, en todo caso, los requisitos de confidencialidad previstos en esta ley.

Se trata, como ya vimos, de un repositorio en el que se deja constancias de todas las comunicaciones recibidas, su tramitación, respuestas, etc. Por ello, por constituir un almacén de información sensible, el citado precepto resalta que este registro no será público y que «únicamente a petición razonada de la Autoridad judicial competente, mediante

auto, y en el marco de un procedimiento judicial y bajo la tutela de aquélla, podrá accederse total o parcialmente al contenido del referido registro».

Por otra parte, el art. 26 contempla otra previsión, en esta ocasión relativa al tiempo de conservación de los datos registrados. Así se establece que los datos personales relativos a las comunicaciones recibidas y a las investigaciones internas a que se refiere el párrafo anterior sólo se conservarán durante el período que sea necesario y proporcionado a efectos de cumplir con la presente ley. En particular, se tendrá en cuenta lo previsto en los apartados tercero y cuarto del artículo 32 (a los que aludiremos a continuación). Fijándose como límite que, en ningún caso, puedan conservarse los datos por un período superior a 10 años.

5.7. Protección de datos

En materia de protección de datos personales debemos destacar dos preceptos.

Por un lado, el art. 32 del Anteproyecto. Este artículo fija, en primer lugar, límites en el acceso de la información albergada en los sistemas internos. Señalándose que únicamente corresponderá a:

a) El responsable del Sistema y a quien lo gestione directamente.

b) El responsable de recursos humanos, sólo cuando pudiera proceder la adopción de medidas disciplinarias contra un trabajador. En el caso de los empleados públicos, el órgano competente para la tramitación del mismo.

c) El responsable de los servicios jurídicos de la entidad u organismo, si procediera la adopción de medidas legales en relación con los hechos relatados en la comunicación.

d) Los encargados del tratamiento que eventualmente se designen.

e) El Delegado de Protección de Datos.

Así también, el apartado segundo de dicho artículo contempla que también será lícito el tratamiento de los datos por otras personas, o incluso su comunicación a terceros, cuando resulte necesario para la tramitación de los procedimientos sancionadores o penales que, en su caso, procedan.

En otro orden de cosas, como se vio, los apartados cuarto y quinto del art. 32 prevén una serie de disposiciones también en materia de conservación de datos. Concretamente, en el apartado tercero se establece que «Los datos que sean objeto de tratamiento podrán conservarse en el

sistema de informaciones únicamente durante el tiempo imprescindible para decidir sobre la procedencia de iniciar una investigación sobre los hechos informados». Y, acto seguido, el apartado cuarto se refiere a que «En todo caso, transcurridos tres meses desde la recepción de la comunicación sin que se hubiesen iniciado actuaciones de investigación, deberá procederse a su supresión, salvo que la finalidad de la conservación sea dejar evidencia del funcionamiento del sistema». Por último, se apunta a que las comunicaciones a las que no se haya dado curso solamente podrán constar de forma anonimizada, sin que sea de aplicación la obligación de bloqueo prevista en el artículo 32 de la Ley Orgánica 3/2018, de 5 de diciembre.

Y, por otro lado, el art. 33 contempla una serie de disposiciones relativas a la preservación de la identidad del informante y de las personas investigadas. En primer lugar, el citado precepto se encarga de proclamar que quien presente una comunicación o lleve a cabo una revelación pública tiene derecho a que su identidad no será revelada a terceras personas. Para ello se establece que los sistemas internos de información, los canales externos y quienes reciban revelaciones públicas deberán contar con medidas técnicas y organizativas adecuadas para preservar la identidad y garantizar la confidencialidad de los datos correspondientes a las personas investigadas por la información suministrada, especialmente la identidad del informante en caso de que se hubiera identificado.

El apartado tercero del art. 33 recoge una cláusula, a nuestro juicio, cuestionable y además contraproducente: «La identidad del informante sólo podrá ser comunicada a la Autoridad judicial, al Ministerio Fiscal o a la autoridad administrativa competente en el marco de una investigación penal, disciplinaria o sancionadora». Que la identidad del denunciante sea necesaria para iniciar o proseguir un determinado procedimiento contra alguien por unos concretos hechos (de los que nadie más tenga conocimiento) es algo que puede asumirse si la ley así lo establece. Ahora bien, también es cierto que en ocasiones poco o nada aporta conocer tal identidad. Dicho lo cual, el potencial informante puede optar por no denunciar o hacerlo de forma anónima si, una vez identificado bajo un régimen de confidencialidad, ésta decae ante un requerimiento judicial o de autoridad administrativa. Esto es, puede querer denunciar, pero, no verse inmerso en un proceso.

Por último, el art. 33 del Anteproyecto impone la obligación de nombrar a un delegado de protección de datos a todas las entidades obligadas a disponer de un sistema interno de comunicaciones, así como los terceros externos que en su caso lo gestionen. Debiendo proceder de igual modo la Autoridad Independiente de Protección del Informante y las autoridades independientes que en su caso se constituyan.

5.8. La Autoridad Independiente de Protección del Informante: aspectos principales

Una de las novedades más importantes que pretende incorporar este Anteproyecto es la creación de un canal externo de comunicaciones confiándoselo a una institución bautizada como «Autoridad Independiente de Protección del Informante». Esto es, un canal ajeno (paralelo) a los internos de las entidades privadas y públicas. El art. 42.1 del citado Anteproyecto la define como una autoridad administrativa independiente como ente de derecho público de ámbito estatal, de las previstas en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, con personalidad jurídica propia y plena capacidad pública y privada, que actuará en el desarrollo de su actividad y para el cumplimiento de sus fines con plena autonomía e independencia orgánica y funcional respecto del Gobierno, de las entidades integrantes del sector público y de los poderes públicos en el ejercicio de sus funciones.

5.8.1. Funciones y ámbito competencial

Tal y como describe el art. 43 del Anteproyecto, entre sus funciones principales se encuentran las de: 1) gestión del canal externo de comunicaciones regulado en el título III; 2) adopción de las medidas de protección al informante previstas en la presente ley; y, 3) tramitación de los procedimientos sancionadores e imposición de sanciones por las infracciones previstas en el título IX. No obstante, la Autoridad tiene otras funciones como las de: 1) participar, mediante informe preceptivo, en el proceso de elaboración de normas que afecten a su ámbito de competencias, a la ley reguladora de sus funciones y su normativa de desarrollo; y, 2) elaboración de recomendaciones y directrices que establezcan los criterios y prácticas adecuados para el cumplimiento de las disposiciones contenidas en la presente ley.

De otra parte, el art. 24 del citado Anteproyecto se encarga de enumerar aquellos supuestos en que se activa la competencia de esta Autoridad (de ámbito nacional), esto es, cuándo le corresponde tramitar las comunicaciones. A este respecto, la mayoría de casos refieren a comunicaciones que afectan a entidades públicas, pero, en el ámbito privado se alude en el art. 24.1.d) a comunicaciones que afecten a «Entidades que integran el sector privado, cuando la infracción o el incumplimiento informado afecte o produzca sus efectos en el ámbito territorial de más de una comunidad autónoma». Y, el apartado 2 del mismo artículo alude a que la Autoridad Independiente u órgano que pueda señalarse en cada comunidad autónoma, «lo será respecto de las informaciones que afecten (…) a las entidades que formen parte del sector privado, cuando el incumplimiento comunicado se circunscriba al ámbito territorial de la correspondiente comunidad autónoma». En este sentido, consideramos

que, si bien en principio la distribución competencial parece razonable, lo cierto es que ello hará (presumiblemente) que un porcentaje muy elevado de las denuncias se dirijan a los órganos autonómicos. Por ello, a nuestro juicio, hubiera sido preferible optar por alguno de estos otros criterios:

— Sujeto denunciado (persona física o jurídica)

— Naturaleza jurídica (empresa, partido político, sindicato, fundación)

— Materias

— Clase de «irregularidad» denunciada.

— Entidad de la conducta reportada.

— Grado de afectación, impacto, repercusión

5.8.2. Aspectos procedimentales

Las cuestiones relativas al procedimiento se encuentran recogidas en los artículos que pasamos a comentar.

A) Recepción de comunicaciones.

El primero de ellos, el art. 17 se encarga de regular la recepción de comunicaciones. El apartado primero permite que la comunicación pueda llevarse a cabo de forma anónima. Y, si no se opta por el anonimato, se reservará la identidad del informante en los términos del artículo 33, debiendo adoptarse las medidas en él previstas. Como dijimos más arriba, ambos sistemas presentan ventajas e inconvenientes. Ahora bien, debemos valorar positivamente que al menos se brinde la oportunidad de implantar canales anónimos. Y, en consecuencia, que se deje a elección del sujeto obligado a dotarse de una u otra clase de sistemas.

En cuanto al formato de la denuncia, el apartado segundo de dicho precepto prevé que puede realizarse por escrito, a través de correo postal o a través de cualquier medio electrónico habilitado al efecto dirigido al canal externo de informaciones de la Autoridad Independiente de Protección del Informante, o verbalmente, por vía telefónica o a través de sistema de mensajería de voz. Además, a solicitud del informante, también podrá presentarse mediante una reunión presencial. Y, en los casos de comunicación verbal se advertirá al informante de que la comunicación será grabada y se le informará del tratamiento de sus datos de acuerdo con lo que establecen el Reglamento (UE) 2016/679 y la Ley Orgánica 3/2018.

Cuando el informante se identifique, al efectuar la comunicación podrá indicar un domicilio, correo electrónico o lugar seguro a efectos de recibir las notificaciones, pudiendo asimismo renunciar expresamente a la recepción de cualquier comunicación de actuaciones llevadas a cabo por la Autoridad Independiente de Protección del Informante como consecuencia de la comunicación.

Y, en caso de comunicación verbal, la Autoridad Independiente de Protección del Informante deberá documentarla de alguna de las maneras siguientes:

a) mediante una grabación de la conversación en un formato seguro, duradero y accesible; o

b) a través de una transcripción completa y exacta de la conversación realizada por el personal responsable de tratarla.

En estos casos, y sin perjuicio de los derechos que le corresponden de acuerdo a la normativa sobre protección de datos, se ofrecerá al informante la oportunidad de comprobar, rectificar y aceptar mediante su firma la transcripción del mensaje.

Por su parte, el apartado tercero prevé que, una vez realizada la comunicación, se proceda a su registro en el Sistema de Gestión de Comunicaciones, siéndole asignado un código de identificación. El Sistema de Gestión de Comunicaciones estará contenido en una base de datos segura y de acceso restringido exclusivamente al personal de la Autoridad Independiente de Protección del Informante convenientemente autorizado, en la que se registrarán todas las comunicaciones recibidas, cumplimentando los siguientes datos:

a) Fecha de recepción.

b) Código de identificación.

c) Actuaciones desarrolladas.

d) Medidas adoptadas.

e) Fecha de cierre.

Por último, tras recibirse la comunicación, en un plazo no superior a cinco días hábiles desde dicha recepción, se procederá a acusar recibo de la misma, a menos que la comunicación sea anónima o el informante expresamente haya renunciado a recibir comunicaciones relativas a la investigación.

B) Admisión

El art. 18.1 contempla que, una vez registrada la comunicación, la Autoridad Independiente de Protección del Informante deberá compro-

bar si aquélla expone hechos o conductas que se encuentran dentro del ámbito de aplicación recogido en el artículo 2 *y si los hechos pudieran ser indiciariamente constitutivos de delito*.

Hemos de destacar este apartado primero del art. 18 porque en el Informe del CGPJ (p. 50) se afirma que «el apartado 1 del artículo 18 se refiere exclusivamente a «hechos indiciariamente constitutivos de delito», debiendo incluirse la referencia a las infracciones administrativas o de Derecho de la Unión Europea, pues el ámbito de aplicación de la Directiva y de la norma proyectada no se limitan a las infracciones penales». Sin embargo, a nuestro juicio, ello no es así, pues, se alude también a «hechos o conductas que se encuentran dentro del ámbito de aplicación recogido en el artículo 2» (entre las que se encuentran las infracciones penales). Así pues, en nuestra opinión, en todo caso, lo que sobra es la referencia explícita a y *si los hechos pudieran ser indiciariamente constitutivos de delito*.

Realizado este análisis preliminar, la Autoridad Independiente de Protección del Informante dispone de un plazo (que no podrá ser superior a diez días hábiles desde la fecha de entrada en el registro de la información) para adoptar alguna de las siguientes decisiones:

a) Inadmitir la comunicación, en alguno de los siguientes casos:

1º. Cuando los hechos relatados carezcan de toda verosimilitud.

2º. Cuando los hechos relatados no sean constitutivos de infracción del ordenamiento jurídico incluida en el ámbito de aplicación de esta ley o, siéndolo, no afecten al interés general.

3º. Cuando la comunicación carezca manifiestamente de fundamento o existan, a juicio de la Autoridad Independiente de Protección del Informante, indicios racionales de haberse obtenido de forma ilícita. En este último caso, siempre que el acceso pudiera ser constitutivo de un delito no perseguible de oficio, además de la inadmisión se deducirá el tanto de culpa o se remitirá al Ministerio Fiscal relación circunstanciada de los hechos que se estimen constitutivos de delito.

4º. Cuando la información sea mera reproducción de otra anterior previamente inadmitida o debidamente investigada.

La inadmisión se comunicará al informante dentro de los cinco días hábiles siguientes, salvo que la comunicación fuera anónima o el informante hubiera renunciado a recibir comunicaciones de la Autoridad Independiente de Protección del Informante.

b) Admitir a trámite la comunicación

La admisión a trámite se comunicará al informante dentro de los cinco días hábiles siguientes, salvo que la comunicación fuera anónima o el informante hubiera renunciado a recibir comunicaciones de la Autoridad Independiente de Protección del Informante.

c) Remitir la comunicación a la autoridad, entidad u organismo que se considere competente para su tramitación o cuando afecte a los intereses de la Hacienda Pública. Cuando los hechos pudieran ser indiciariamente constitutivos de delito, se remitirá al Ministerio Fiscal.

C) Instrucción

El art. 19.1 del Anteproyecto establece que la instrucción comprenderá todas aquellas actuaciones encaminadas a comprobar la verosimilitud de los hechos relatados. Establecido en estos términos, el art. 19.1 parece conferir plenitud de poderes a la Autoridad para realizar cualquier tipo de averiguación. Dichas innominadas posibilidades de actuación son contrarias al principio de legalidad. Por ello sería recomendable que, al menos vía reglamentaria, se delimitasen las facultades de investigación que se atribuyen a la Autoridad.

Tan solo el apartado tercero parece referirse a uno de esos medios: «(…) la instrucción comprenderá, siempre que sea posible, una entrevista con la persona investigada en la que, siempre con absoluto respeto a la presunción de inocencia, se le invitará a exponer su versión de los hechos y a aportar aquellos medios de prueba que considere adecuados y pertinentes (…)».

Por último, debemos reparar en la dicción que presenta el apartado quinto: «Todas las personas naturales o jurídicas, privadas o públicas, deberán colaborar con las autoridades competentes y estarán obligadas a atender los requerimientos que se les dirijan para aportar documentación, datos o cualquier información relacionada con los procedimientos que se estén tramitando, incluso los datos personales que le fueran requeridos».

Este último apartado, debe ponerse en relación con el art. 63.3 que considera infracción leve (respectivamente):

a) la remisión de información de forma incompleta, de manera deliberada por parte del Responsable del Sistema a la Autoridad, o fuera de plazo; y,

b) el incumplimiento de la obligación de colaboración con la investigación de informaciones.

Aquí, como sucede por ejemplo en el delito fiscal, se plantea la polémica cuestión de si la previa colaboración en sede administrativa (bajo apercibimiento de sanción) no conculca el derecho a no autoincriminarse cuando éste pretenda invocarse posteriormente en el proceso penal. Con todo, si bien el TEDH así lo ha considerado en numeras ocasiones, nuestro Tribunal Constitucional parece inclinarse más bien, desde hace tiempo, por la tesis contraria (no viendo conculcación del citado derecho

en estos supuestos)[43]. Personalmente, en nuestro ámbito, entendemos que las «pruebas» (autoinculpatorias) obtenidas bajo coacción que, posteriormente, se pretendieran hacer valer en un proceso penal, debieran ser expulsadas del mismo de inmediato (no pudiéndose tomar en consideración).

D) Terminación de las actuaciones

El art. 20 del Anteproyecto contempla que, una vez concluidas todas las actuaciones, la Autoridad Independiente de Protección del Informante emitirá un informe que contendrá al menos:

a) Una exposición de los hechos relatados junto con el código de identificación de la comunicación y la fecha de registro.

b) La clasificación de la comunicación a efectos de conocer su prioridad o no en su tramitación.

c) Las actuaciones realizadas con el fin de comprobar la verosimilitud de los hechos,

d) Las conclusiones alcanzadas en la instrucción y la valoración de las diligencias y de los indicios que las sustentan.

Emitido el informe, la Autoridad Independiente de Protección del Informante adoptará alguna de las siguientes decisiones:

a) Archivo del expediente, que será comunicado al informante y, en su caso, y a la persona investigada. En estos supuestos, el informante tendrá derecho a la protección prevista en la presente ley, salvo que, como consecuencia de las actuaciones llevadas a cabo en fase de instrucción, se concluyera que la información a la vista de la información recabada, debía haber sido inadmitida por concurrir las causas previstas en el artículo 18.2 a).

b) Remisión al Ministerio Fiscal si, pese a no apreciar inicialmente indicios de que los hechos pudieran revestir el carácter de delito, así resultase del curso de la instrucción. Si el delito afectase a los intereses financieros de la Unión, lo remitirá a la Fiscalía Europea.

c) Traslado de todo lo actuado a la autoridad competente, de conformidad con lo dispuesto en el artículo 18.2.c).

d) Adopción de acuerdo de inicio de un procedimiento sancionador en los términos previstos en el título IX.

[43] *Vid.*, en cuanto a las referencias jurisprudenciales, Hermosín Álvarez, M.: «Los derechos de defensa y el deber de colaboración con la administración tributaria», *Estudios de Deusto*, núm. 66-2, 2018, pp. 226 y ss.

El art. 20 prevé, además, que «En todo caso, el plazo para finalizar las actuaciones y dar respuesta al informante, en su caso, no podrá ser superior a tres meses desde la entrada en registro de la comunicación. Cualquiera que sea la decisión, además del archivo, se comunicará al informante, salvo que haya renunciado a ello o que la comunicación sea anónima». Hemos de destacar esta previsión porque en ella se fija un plazo para finalizar las actuaciones y dar respuesta al informante que no podrá ser superior a tres meses. Sin embargo, debemos advertir que la propia Directiva europea, en su art. 11.2 d) alberga la posibilidad de ampliar dicho plazo a seis meses «en casos debidamente justificados». El Informe del CGPJ advierte también de este desfase (p. 48), pero, no propone (salvo error u omisión por nuestra parte) que dicha contradicción debiera corregirse.

5.9. Revelación pública

En último lugar, el Anteproyecto prevé la figura de la «revelación pública». Esto es, «*la puesta a disposición del público de información sobre acciones u omisiones en los términos previstos en la presente ley*» (art. 27.2). Para las personas que hagan una revelación pública, el Anteproyecto contempla en el art. 28 un régimen de protección, pero, solo cuando se den las siguientes circunstancias:

a) Que haya realizado la comunicación primero por canales internos y externos, o directamente por canales externos, de conformidad con los títulos II y III, sin que se hayan tomado medidas apropiadas al respecto en el plazo establecido.

b) Que tenga motivos razonables para pensar que:

   i) la infracción puede constituir un peligro inminente o manifiesto para el interés público, en particular cuando se da una situación de emergencia, o existe un riesgo de daños irreversibles, incluido un peligro para la integridad física de una persona, o

   ii) en caso de comunicación a través de canal externo, exista un elevado riesgo de represalias o haya pocas probabilidades de que se dé un tratamiento efectivo a la información debido a las circunstancias particulares del caso.

5.10. Infracciones y sanciones

En virtud del art. 63,

"Tendrán la consideración de infracciones muy graves las siguientes acciones u omisiones:

a) Cualquier actuación que suponga una efectiva limitación de los derechos y garantías previstos en la presente ley introducida a través de contratos o acuerdos a nivel individual o colectivo y en general cualquier intento o acción efectiva de obstaculizar la presentación de comunicaciones o de impedir, frustrar o ralentizar su seguimiento, incluida la aportación dolosa de información o documentación falsa por parte de los requeridos para ello.

b) La adopción de cualquier represalia frente a los informantes derivada de la comunicación.

c) Vulnerar las garantías de confidencialidad y anonimato previstas en esta ley, y de forma particular cualquier acción u omisión tendente a revelar la identidad del informante cuando este haya optado por el anonimato, aunque no se llegue a producir la efectiva revelación de la misma.

d) Vulnerar el deber de mantener secreto sobre cualquier aspecto relacionado sobre la información.

e) La comisión de una infracción grave cuando el autor hubiera sido sancionado mediante resolución firme por dos infracciones graves en los dos años anteriores a la comisión de la infracción, contados desde la firmeza de las sanciones.

f) Comunicar o revelar públicamente información a sabiendas de su falsedad, en las comunicaciones en las que se identifique el informante.

Tendrán la consideración de infracciones graves las siguientes acciones u omisiones:

a) Cualquier actuación que suponga limitación de los derechos y garantías previstos en la presente ley o cualquier intento o acción efectiva de obstaculizar la presentación de informaciones o de impedir, frustrar o ralentizar su seguimiento que no tenga la consideración de infracción muy grave conforme al apartado 1 anterior.

b) Vulnerar las garantías de confidencialidad y anonimato previstas en esta ley cuando no tenga la consideración de infracción muy grave.

c) Vulnerar el deber de secreto en los supuestos en que no tenga la consideración de infracción muy grave.

d) Incumplimiento de la obligación de adoptar las medidas para garantizar la confidencialidad y secreto de las informaciones.

e) La comisión de una infracción leve cuando el autor hubiera sido sancionado por dos infracciones leves en los dos años anteriores a la comisión de la infracción, contados desde la firmeza de las sanciones.

Tendrán la consideración de infracciones leves las siguientes acciones u omisiones:

a) Remisión de información de forma incompleta, de manera deliberada por parte del Responsable del Sistema a la Autoridad, o fuera del plazo concedido para ello.

b) Incumplimiento de la obligación de colaboración con la investigación de informaciones.

c) Cualquier incumplimiento de las obligaciones previstas en esta ley que no esté tipificado como infracción muy grave o grave».

Más allá de cuestionar la dudosa técnica que supone tipificar las infracciones graves «cuando no tengan la consideración de infracción muy grave», nos sorprende que el hecho de no implantar los canales de denuncia cuando se esté obligado a ello no suponga infracción alguna, pues, no se recoge en el catálogo de infracciones (defecto que ya advertimos en la Directiva europea). Esta afirmación se nos podría rebatir arguyendo que la primera de las infracciones muy graves alude a «cualquier actuación que suponga una efectiva limitación de los derechos y garantías previstos en la presente ley»; y, claro está, la posibilidad de denunciar es uno de ellos. Por tanto, no establecer un canal de denuncias conculcaría tal derecho. Sin embargo, no podemos obviar que a continuación se dice «introducida a través de contratos o acuerdos a nivel individual o colectivo», lo cual nos da la razón, pues, no está pensando en incumplir la obligación de incorporar tales mecanismos. Pero es que, también entre las infracciones muy graves se encuentra «en general cualquier intento o acción efectiva de obstaculizar la presentación de comunicaciones». Pero, una vez más, a nuestro juicio, consideramos que impedir o intentar impedir las denuncias es una conducta que parte de una premisa (que haya canal de denuncias) y se lleve a cabo una actividad obstaculizadora para que no se utilice (no que se obstaculice por no contar con un canal).

Por último, también es cierto que, entre las infracciones leves expresamente se recoge: «cualquier incumplimiento de las obligaciones previstas en esta ley que no esté tipificado como infracción muy grave o grave». Y la obligación de dotarse de estos mecanismos (así recogida en el texto legal) no está catalogada como tal ni en las infracciones muy graves ni en las graves. Pero, a este razonamiento debemos objetar que, resultaría paradójico que la infracción más grave (no implantar el canal interno) fuera considerada de «menor entidad» (pues se consideraría leve) que las formalmente previstas como muy graves o graves, que no alcanzarían, a nuestro juicio, la gravedad que comporta no dotarse de tales sistemas.

Y, en virtud del art. 65,

1. La comisión de infracciones previstas en esta ley llevará aparejada la imposición de las siguientes multas:

a) Si son personas físicas las responsables de las infracciones, serán multadas con una cuantía de hasta 10.000 euros por la comisión de infracciones leves; de 5.001 hasta 30.000 euros por la comisión de infracciones graves y de 30.001 hasta 300.000 euros por la comisión de infracciones muy graves.

b) Si son personas jurídicas serán multadas con una cuantía hasta 100.000 euros en caso de infracciones leves, entre 100.001 y 600.000 euros en caso de infracciones graves y entre 600.001 y 1.000.000 euros en caso de infracciones muy graves.

2. Adicionalmente, en el caso de infracciones muy graves, la Autoridad Independiente de Protección del Informante podrá acordar:

a) La amonestación pública.

b) La prohibición de obtener subvenciones u otros beneficios fiscales durante un plazo máximo de cuatro años.

c) La prohibición de contratar con el sector público durante un plazo máximo de tres años de conformidad con lo previsto en la Ley 9/2017 de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014.

3. Las sanciones por infracciones muy graves de cuantía igual o superior a seiscientos mil euros impuestas a entidades jurídicas podrán ser publicadas en el Boletín Oficial del Estado.

En cuanto a la prohibición de obtener subvenciones u otros beneficios fiscales, el CGPJ, en su Informe de 26 de mayo de 2022, señalaba que «el precepto proyectado debería limitar la medida de privación de obtener subvenciones u otros beneficios fiscales durante un plazo máximo de cuatro años al ámbito propio regulado por la Ley, esto es, a aquellas subvenciones y beneficios fiscales vinculados a la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción». Con todo, no entendemos bien a qué se quiere referir el citado órgano con lo de *vinculados a la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción*. Ni tampoco, porqué debiera ser así.

6. A modo de reflexión final

Después de haber hecho un repaso por los principales aspectos que se suscitan en torno a los canales de denuncia, debemos advertir que, bien de forma incentivada (para lograr a través de los programas de cumplimiento la exención prevista en el Código Penal); o, coactiva (bajo apercibimiento de sanción como prevé el Anteproyecto), el uso efectivo

de estos mecanismos puede ser menos frecuente de lo que *a priori* (imbuidos por un espíritu pro denuncia) cupiere esperar. Así, las expectativas inicialmente generadas en torno a las bondades de estos sistemas pueden verse rápidamente frustradas por algunos de los factores o circunstancias vistas en este trabajo. En este sentido, a pesar de los pasos dados por el legislador desde la introducción del régimen de responsabilidad penal de las personas jurídicas, cabría poner de manifiesto que los cambios culturales (y éste, el de «denunciar», lo es)[44] no se consiguen de hoy para mañana y, menos, a golpe de norma. Por ello, el éxito o fracaso que dichas herramientas tengan en un futuro es impredecible, pero, de lo que estamos convencidos es que la confianza en los canales de denuncia corporativos solo puede conseguirse: a través de una adecuada y efectiva protección del denunciante; de las garantías que rodeen al procedimiento de comunicación; de la configuración que se le dé (más o menos compleja) al canal; de su funcionamiento real; de las consecuencias que finalmente tenga el haber denunciado tanto para quien señala como para quien se ve señalado; del coste de oportunidad que se le presenta a quien pretende informar de unos hechos (con posible relevancia penal) en los que haya participado (en cuyo caso su responsabilidad solo se verá aminorada a través de figuras como la atenuante de colaboración o el indulto)[45]; etc.

Habrá que esperar, pues, para comprobar cuál es la acogida que con el paso del tiempo tengan estos instrumentos de delación (para la prevención y/o represión de conductas irregulares/delictivas) en el sector privado. Del mismo modo que, algo que ahora nos parece tan extraño a nuestra tradición jurídica como el de recompensar no solo económicamente (bien por parte de la propia empresa o del Estado) a quien esté dispuesto a denunciar, se convierta en algo «natural» dentro de un tiempo. Incluso, que ésta se convierta en la única forma (o una de las principales) que despierte en los empleados, directivos, ciudadanos, etc., la conciencia de denunciar.

En definitiva, en la medida de nuestras posibilidades, hemos tratado de aportar las claves prácticas que deberían regir la implementación de estos mecanismos en el ámbito corporativo privado. No debiéndose olvidar que, tanto en lo relativo a su integración como un elemento esencial de los sistemas de *compliance*, como en la recién obligación contenida en el Anteproyecto, son muchas las dudas (o sombras) que

[44] En este sentido, no puede afirmarse que, con carácter general, la delación forme parte de nuestra cultura, a diferencia de lo que ocurre en otras sociedades o sistemas jurídicos.

[45] A este respecto, véase la interesante propuesta que plantea Simón Castellano para evitar la sanción penal del whistlebower que denuncia unos hechos delictivos en los que puede haber intervenido. Simón Castellano, P.: «La inmunidad penal como recompensa a los denunciantes. Allende un nuevo factor subjetivo-formal de punibilidad», *Revista Electrónica de Ciencia Penal y Criminología*, 2022, núm. 24-14, pp. 1-32.

afloran, deseando que la práctica corporativa, el desarrollo normativo y la jurisprudencia se encarguen de ir despejándolas con el paso del tiempo. Esperemos, ¡eso sí¡, que sea siempre para aportar mayor seguridad jurídica y no lo contrario. En este sentido, como se ha hecho hincapié, son varios los aspectos del Anteproyecto los que debieran corregirse: rehuir de formulaciones excesivamente amplias; de concesión de amplias facultades de comprobación a las Autoridades responsables de los canales externos; de solventar las fricciones apuntadas con respecto de la norma europea; y, sobre todo, de iniciar una fase de reglamentación, especialmente, de todas las cuestiones procedimentales que se recogen en la futura Ley.

Asimismo, anotar que, en la actualidad, la tecnología es ya un aliado natural en el diseño, implementación, gestión y revisión de los *compliance*[46]. Pero, más allá de esta constatación, la Inteligencia Artificial y, particularmente, la tecnología blockchain están llamados a jugar un papel decisivo en el funcionamiento de los canales de denuncia, aspecto (de entre todos los que integran un compliance) sobre el que pueden tener una proyección especial[47]. Piénsese en funcionalidades como: a) llevar a cabo un primer cribado en la admisión de denuncias; b) detectar una falta de fundamentación en las misma; c) seleccionar la información relevante: d) calificar «jurídicamente» los hechos denunciados; e) proponer acciones (archivo, elevar una propuesta de sanción, posible incriminación de la persona jurídica, presentación de querella o denuncia, confesión, colaboración con las autoridades, etc.); entre otras.

Por último, quisiéramos poner de relieve que la creación de organismo públicos como los que pretende este Anteproyecto (y a los que alude la Directiva) y otros autonómicos de cariz similar requieren de un acompañamiento presupuestario sin el cual el correcto funcionamiento de estas nuevas instituciones está abocado al fracaso (¡el tiempo dirá!). En este sentido, dotar de suficientes medios materiales y técnicos es primordial, al igual que nutrirse de un personal altamente cualificado para ello. De igual modo, la imparcialidad de dichos organismos no puede verse cuestionada. De ahí que resulta esencial que no sean instituciones politizadas (o lo mínimo posible), que no sean utilizadas (instrumentalizadas) con fines políticos, especialmente, en casos de corrupción, etc.

---

[46] *Vid.* ampliamente, sobre esta cuestión, León Alapont, *Compliance Penal…*, *op. cit*., p. 349 y ss.

[47] *Vid.*, con mayor detalle, Navarro Cardoso, F.: «*Blockchain, Smart Contract y Compliance*: Anotaciones para el Derecho Penal y Procesal de la persona jurídica», en Demetrio Crespo, E. (Dir.): *Derecho penal y Comportamiento Humano. Avances desde la Neurociencia y la Inteligencia Artificial*, Valencia, Tirant lo Blanch, 2022, p. 681 y 687 y ss.

7. Bibliografía

Abel Souto, M.: «Algunas discordancias legislativas sobre la responsabilidad criminal de las personas jurídicas en el código penal español», *Revista General de Derecho Penal*, núm. 35, 2021, pp. 1-62.

Aránguez Sánchez, C.: «El diseño de programas de prevención de delitos para personas jurídicas», *Revista Electrónica de Ciencia Penal y Criminología*, 2020, núm. 22-20, pp. 1-26.

Bachmaier Winter, L.: «Whistleblowing europeo y compliance: La Directiva EU de 2019 relativa a la protección de personas que reporten infracciones del Derecho de la Unión», *Diario La Ley*, núm. 9539, 2019, pp. 1-10.

Casanovas Ysla, A.: «La norma UNE 19601 y los requisitos del Código Penal», en Gómez-Jara Díez, C. (Coord.): *Persuadir y Razonar: Estudios Jurídicos en Homenaje a José Manuel Maza Martín. Tomo II*, Cizur Menor, Thomson Reuters-Aranzadi, 2018, pp. 887-916.

Díaz Aldao, M. y Hernández Pérez, E.: «Las investigaciones internas del modelo de prevención penal», en GÓMEZ-JARA DÍEZ, C. (Coord.): *Persuadir y Razonar: Estudios Jurídicos en Homenaje a José Manuel Maza Martín. Tomo II*, Cizur Menor, Thomson Reuters-Aranzadi, 2018, pp. 989-1015.

Etxeberria Bereziartua, E.: ««Whistleblowing» o canales de denuncia: La garganta profunda de las empresas», *Diario La Ley*, núm. 9342, 2019, pp. 1-16.

Galán Muñoz, A.: «Whistleblowing anónimo y compliance penal tras la aprobación de la Ley Orgánica 3/2018, de Protección de Datos personales y de garantía de los derechos digitales: una decisión político-criminal a revisar», en Colomer Hernández, I. (Dir.): Uso y cesión de evidencias y datos personales entre procesos y procedimientos sancionadores o tributarios, Cizur Menor, Thomson Reuters-Aranzadi, 2019, pp. 239-261.

— «¿Cultura o estructura? ¿esa es la cuestión? La difícil convivencia y coordinación de los dos sistemas de tratamiento penal de las personas jurídicas en el ordenamiento español», *Revista General de Derecho Penal*, núm. 35, 2021, pp. 1-33.

Gimeno Beviá, J.: *Compliance y proceso penal. El proceso penal de las personas jurídicas*, Cizur Menor, Thomson Reuters-Aranzadi, 2016.

— «De falciani a birkenfeld: la evolución del delator en un cazarrecompensas. Aspectos procesales e incidencia frente a las personas jurídicas (whistleblower vs bounty hunter)», *Diario La Ley*, núm. 9139, 2018.

— «Whistleblowing y proceso penal: una lectura desde las garantías procesales», en Olaizola Nogales, I.; Sierra Hernaiz, E. Y López Ló-

pez, H. (Dirs.): *Análisis de la Directiva UE 2019/1937, Whistleblower desde las perspectivas penal, procesal laboral y administrativo-financiera*, Cizur Menor, Thomson Reuters-Aranzadi, 2021, pp. 161-178.

Gómez-Jara Díez, C.: «La culpabilidad de la persona jurídica», en Bajo Fernández, M.; Feijóo Sánchez, B. Y Gómez-Jara Díez, C.: *Tratado de responsabilidad penal de las personas jurídicas*, Cizur Menor, Thomson Reuters-Aranzadi, 2016, pp. 143-219.

Gómez Tomillo, M.: *Compliance penal y política legislativa. El deber personal y empresarial de evitar la comisión de ilícitos en el seno de las personas jurídicas*, Valencia, Tirant lo Blanch, 2016.

Goñi Sein, J. L.: «Criminalidad de empresa, mecanismos de denuncia o *whistleblowing* y protección de datos», en AA.VV: *Derecho de la empresa y protección de datos*, Cizur Menor, Thomson Reuters-Aranzadi, 2008, pp. 21-65.

— «Programas de cumplimiento empresarial (*compliance programs*): aspectos laborales», en Mir Puig, S.; Corcoy Bidasolo, M. Y Gómez Martín, V.: *Responsabilidad de la empresa y compliance. Programas de prevención, detección y reacción penal*, Montevideo-Buenos Aires, B de F, 2013, p. 401.

Hermosín Álvarez, M.: «Los derechos de defensa y el deber de colaboración con la administración tributaria», *Estudios de Deusto*, núm. 66-2, 2018, pp. 219-248.

León Alapont, J.: «Partidos políticos y responsabilidad penal de las personas jurídicas: consideraciones en torno a su régimen jurídico y los *compliances programs*», en Matallín Evangelio, Á. (Dir.), *Compliance y prevención de delitos de corrupción*, Valencia, Tirant lo Blanch, 2018, pp. 153-191.

— *La responsabilidad penal de los partidos políticos*, Valencia, Tirant lo Blanch, 2019.

— «*Criminal compliance*: análisis de los arts. 31 bis 2 a 5 y 31 quater CP», *Revista General de Derecho Penal*, núm. 31, 2019, pp. 1-36.

— «Retos jurídicos en el marco de las investigaciones internas corporativas: a propósito de los *compliances*», *Revista Electrónica de Ciencia Penal y Criminología*, núm. 22-04, 2020, pp. 1-34.

— *Compliance Penal. Especial referencia a los partidos políticos*, Valencia, Tirant lo Blanch, 2020.

Maroto Calatayud, M.: *La financiación ilegal de los partidos políticos: un análisis político-criminal*, Madrid, Marcial Pons, 2015.

Maza Martín, J. M.: *Delincuencia electoral y responsabilidad penal de los partidos políticos*, Las Rozas, La Ley-Wolters Kluwer, 2018.

Navarro Cardoso, F.: «*Blockchain, Smart Contract y Compliance*: Anotaciones para el Derecho Penal y Procesal de la persona jurídica», en

Demetrio Crespo, E. (Dir.): *Derecho penal y Comportamiento Humano. Avances desde la Neurociencia y la Inteligencia Artificial*, Valencia, Tirant lo Blanch, 2022, pp. 673-697.

Olaizola Nogales, I.; Sierra Hernaiz, E. Y López López, H. (Dirs.): *Análisis de la Directiva UE 2019/1937, Whistleblower desde las perspectivas penal, procesal laboral y administrativo-financiera*, Cizur Menor, Thomson Reuters-Aranzadi, 2021.

Ortiz Pradillo, J. C.: *Los delatores en el proceso penal. Recompensas, anonimato, protección y otras medidas para incentivar una colaboración eficaz con la justicia*, Madrid, Wolters Kluwer-La Ley, 2018.

Palma Herrera, J. M.: «Presupuestos jurídico-penales de la responsabilidad penal de los entes corporativos y del sistema de "compliances"», en Palma Herrera, J. M. Y Aguilera Gordillo, R.: *Compliances y responsabilidad penal corporativa*, Cizur Menor, Thomson Reuters-Aranzadi, 2017, pp. 15-73.

Puyol Montero, J.: *El funcionamiento práctico del canal de compliance «whistleblowing»*, Valencia, Tirant lo Blanch, 2017.

Ragués I Vallés, R.: «Denuncias de los trabajadores ("whistleblowing")», en Ayala Gómez, I. y Ortiz De Urbina Gimeno, I. (Coords.): *Penal económico y de la empresa*, Madrid, Francis Lefebvre, 2016, pp. 200-206.

— «Un nuevo avance en la estandarización de los modelos de prevención de delitos: la ISO 37002 sobre gestión de sistemas de denuncia», *La Ley Compliance penal*, núm. 7, 2021, pp. 1-9.

Simón Castellano, P.: «La inmunidad penal como recompensa a los denunciantes. Allende un nuevo factor subjetivo-formal de punibilidad», *Revista Electrónica de Ciencia Penal y Criminología*, 2022, núm. 24-14, pp. 1-32.