

## EL CANAL DE DENUNCIAS PÚBLICO COMO OPORTUNIDAD PARA UNA NUEVA RELACIÓN ENTRE LA ADMINISTRACIÓN Y EL CIUDADANO

Blanca ARES GONZÁLEZ

Letrada de los Servicios Jurídicos de Castilla y León  
Investigadora de la Universidad de Salamanca

### INTRODUCCIÓN

En un contexto en el que la ciudadanía demanda la prestación de auténticos servicios públicos de calidad y exige comportamientos ejemplares en la gestión de los asuntos públicos, la incorporación de enfoques ajenos a los de los clásicos instrumentos de intervención y la innovación administrativa resultan necesarios para desplegar una auténtica administración del siglo XXI.

El uso inteligente del conocimiento y de la información disponible se torna esencial para mejorar esta relación entre las instituciones y los ciudadanos y, en particular, en el ámbito de las políticas de integridad, los canales de denuncia aparecen como herramientas novedosas capaces de reforzar y fortalecer estos vínculos.

A pesar de que la conocida como Directiva *whistleblower*, a partir de su publicación en el año 2019, generalizó el establecimiento de canales de denuncia en todas las entidades públicas y privadas, su obligatoriedad no se ha trasladado al ordenamiento jurídico español hasta su transposición en 2023. No obstante, la llegada masiva de fondos europeos *Next Generation EU* a través del Mecanismo de Recuperación y Resiliencia y la consecuente obligación para todas las entidades receptoras o ejecutoras de estos fondos de contar con un Plan de Medidas Antifraude ha supuesto, desde nuestro punto de vista, un gran impulso para su implantación definitiva.

La pretensión de este trabajo de investigación no es otra que la de ayudar a las administraciones públicas en su cometido de diseñar e implantar canales de denuncia de manera eficaz y comprometida al tiempo que se esfuerzan en consolidar una cultura ética de cumplimiento en el seno de sus organizaciones.

Para ello, una vez analizado el marco normativo vigente en España, desde las disposiciones de la Directiva *whistleblower* y la Ley 2/2023, de 20 de febrero, *reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción*, hasta los Planes de Medidas Antifraude del Plan de Recuperación, Transformación y Resiliencia de España, extraeremos la experiencia resultante de años de práctica en el sector público, tomando como referencia el trabajo realizado por la Agencia de Prevención y Lucha contra el Fraude y la Corrupción de la Comunitat Valenciana y en el sector privado a través del trabajo de estandarización de las normas ISO para terminar, sobre la base de todo lo anterior, con la formulación de un catálogo de principios generales de aplicación a cualquier entidad pública en su cometido de diseñar e implantar canales de denuncia eficaces para la prevención y detección de irregularidades y casos de fraude.

### I. MARCO CONTEXTUAL: LA IMPORTANCIA DE LA INNOVACIÓN ADMINISTRATIVA EN LA NUEVA GESTIÓN PÚBLICA

Las administraciones públicas se encuentran, desde hace décadas, en un proceso continuo de cambio dirigido a mejorar su rendimiento, ofrecer servicios públicos de calidad a la ciudadanía y a crear valor público, económico y social, en entornos cada vez más inestables.

La sociedad actual reclama, no solo una administración pública que sirva con objetividad a los intereses generales y actúe de acuerdo con los principios de eficacia, jerarquía, descentralización, desconcentración y coordinación, con sometimiento pleno a la ley y al Derecho, como reza el artículo 103 de la Constitución Española, sino que además sea capaz de actuar de forma ágil y gestionar lo público con eficiencia y transparencia.

En definitiva, una administración responsable e inteligente, libre de conflictos de intereses y de riesgo de corrupción, preocupada por la mejora de la calidad de vida y del bienestar colectivo, cercana y que escucha a los ciudadanos en sus demandas e inquietudes<sup>1</sup>.

Desde hace una década que los estudios sobre reforma de la Administración Pública promovidos por el Instituto Nacional de Administraciones Públicas (INAP) nos ilustraban que una gestión inteligente de lo público dirigida a mejorar la prestación de servicios públicos, su eficiencia, cobertura y equidad o a la creación de externalidades positivas en el resto de la economía y de la sociedad implicaba la implementación de mecanismos de innovación administrativa<sup>2</sup>.

RIVERO ORTEGA<sup>3</sup> nos recuerda que esta innovación supone la búsqueda de soluciones creativas o diferentes a los problemas sociales, pudiendo incluir la creación de nuevos servicios, formas de organización, mejoras de procesos o modificaciones de conducta de los ciudadanos.

El principio de innovación, consagrado a nivel europeo, promueve una regulación y unas políticas públicas inteligentes y orientadas al futuro. La actuación de las administraciones públicas debe basarse en una aproximación holística que permita visualizar diferentes contextos de futuro a tener en cuenta para la adopción de decisiones y en una mejor regulación, tal y como marcan los postulados de la gobernanza anticipatoria<sup>4</sup>.

No podemos conformarnos con seguir aplicando viejas recetas en un mundo de vertiginosos cambios y de entornos inestables, necesitamos una auténtica administración inteligente, como nos señalan DÍAZ MÉNDEZ y CUÉLLAR MARTÍN<sup>5</sup>, abierta a procesos de innovación constantes en los que la sociedad desempeñe un papel protagonista. Esta administración se caracteriza por ser sensible a los impactos que provoca su actividad y por aprovechar esta información para mejorar y generar conocimiento. Y añaden que “las administraciones resolutorias y con capacidad de actuación son las que marcan la diferencia: no postergan las decisiones difíciles, sino que las toman buscando las mejores alternativas y tratando de anticiparse a los problemas”<sup>6</sup>.

La administración inteligente necesita incorporar enfoques novedosos que provengan tanto de la gestión pública como de la privada con el objetivo de renovar su capacidad de acción y de innovación y a pesar del riesgo y de la incertidumbre que suponen nuevas formas de actuación.

El concepto *smart governance* —o gobernanza pública inteligente—, analizado en profundidad por CRIADO GRANDE<sup>7</sup> y otros autores dedicados al estudio de la innovación administrativa, recoge los postulados que deben confluir en la gestión pública contemporánea que necesariamente se basan en una gestión pública más abierta, participativa y relacional<sup>8</sup>.

---

<sup>1</sup> Para conocer en detalle los retos a los que se enfrenta el sector público se puede consultar el Informe: “¿En qué hay que transformar la Administración Pública española? Como afrontar el reto del cambio en el sector público”, consultado el 20 de junio de 2023 en *Transformar Administración Pública [pvc.es]*.

<sup>2</sup> De entre todos los trabajos del INAP destaca el realizado por el Grupo de Investigación en Administración Pública 2032 GIAP, recopilado por ARENILLA SÁEZ (2014).

<sup>3</sup> RIVERO ORTEGA (2017).

<sup>4</sup> Para profundizar en las implicaciones del principio de innovación y su relación con las “regulaciones de futuro” promovidas desde las instituciones europeas, es muy recomendable consultar el documento *The Innovation Principle, European Commission, Research and Innovation Department*, 2019, consultado en [https://research-and-innovation.ec.europa.eu/system/files/2022-07/ec\\_rtd\\_factsheet-innovation-principle.pdf](https://research-and-innovation.ec.europa.eu/system/files/2022-07/ec_rtd_factsheet-innovation-principle.pdf).

<sup>5</sup> DÍAZ MÉNDEZ y CUÉLLAR MARTÍN (2007).

<sup>6</sup> Los autores se han dedicado al estudio de la gestión pública y a la propuesta de soluciones y fórmulas de mejora a partir del concepto de “Administración Inteligente” como la reflexión contenida en el párrafo de esta nota.

<sup>7</sup> CRIADO GRANDE (2016).

<sup>8</sup> Merece la pena detenerse en el análisis que nos presenta CRIADO GRANDE (2016), donde expone cuatro casos de innovación administrativa en relación con, por un lado, el *crowdsourcing* ciudadano, analizando las plataformas

La clásica distinción de los modos de intervención administrativa que diferenciaba entre modos formalizados (actos, reglamentos, planes o contratos) y la actividad material o técnica se encuentra hoy superada por los profundos cambios socioeconómicos de las últimas décadas y por la irrupción definitiva de la tecnología debiendo considerarse como habituales ya otras formas de intervención como la autorregulación, la colaboración público-privada, las decisiones consensuadas, el *soft law* o las nuevas fórmulas de participación ciudadana, como la gobernanza anticipatoria o *foresight*<sup>9</sup>.

La complejidad de los problemas actuales, denominados retorcidos o *wicked-problems*, requiere plurales puntos de vista y diversas maneras de abordarlos, más allá del clásico análisis organizativo interno de la gestión pública, basadas en el mayor uso posible del conocimiento científico disponible en red, además de interdisciplinarios y abiertos, según BERNSTEIN<sup>10</sup>.

La incertidumbre es quizás la principal característica de la actual sociedad del riesgo, expresión acuñada originariamente por BECK (1999), lo que conduce a la necesidad por parte de las instituciones, organizaciones e individuos de manejar, forma sistemática, los riesgos e inseguridades generados por las transformaciones experimentadas en las sociedades contemporáneas.

Las diversas metodologías de predicción mediante escenarios, utilizadas desde hace varias décadas por el sector privado, sirven para seleccionar futuros potenciales, comprender mejor las circunstancias que pueden devenir e influir estratégicamente sobre ellas. Como señalan SÁNCHEZ MACÍAS y RODRÍGUEZ LÓPEZ<sup>11</sup>, en este contexto de riesgo e incertidumbre, los estándares, los compendios de buenas prácticas, las certificaciones y el conocimiento experto se presentan como soluciones más o menos simplificadas que permiten tomar decisiones razonables y responsables<sup>12</sup>.

La dogmática jurídica debe preocuparse por las consecuencias sociales de las soluciones propuestas, atender a la experiencia comparada, interdisciplinaria y compartida apostando por el “derecho en acción”, como lo denomina ATIENZA RODRÍGUEZ<sup>13</sup>. Una visión centrada en la proactividad hacia el ciudadano, la automatización inteligente, el gobierno del dato o el cambio cultural son algunos de los ejes sobre los que desarrollar este modelo<sup>14</sup>.

“Los datos, su conversión en conocimiento y su difusión en red son presupuestos del concepto de inteligencia, entendida como memoria de trabajo aplicable a la resolución de problemas. Proyectando estas teorías sobre la organización y los procedimientos de la Administración pública, sabremos cómo conseguir la información y convertirla en conocimiento aplicado, para ponerlo en valor” señala RIVERO ORTEGA<sup>15</sup>, si bien lo importante debe ser seleccionar la información más relevante para evitar los errores a los que nos puede inducir el uso masivo de información detallada sin control, como nos apunta el mismo autor en estudios más recientes<sup>16</sup>.

La administración pública tiene, hoy en día gracias a la generalización de las comunidades de aprendizaje y a la puesta en marcha de procesos de innovación social, la posibilidad de utilizar el conocimiento que los usuarios disponen para aumentar el nivel o la calidad de los servicios que prestan, procesar toda la información disponible gracias a la colaboración de personas y entidades fuera de los márgenes organizativos, incorporar las buenas prácticas observadas en otros entornos

---

*Challenge.gov* y *SantanderCityBrain*, y, por otro, la colaboración abierta entre empleados públicos, analizando las plataformas *GitHub* y *NovaGob*.

<sup>9</sup> PONCE SOLÉ (2018) detalla estas nuevas interacciones, si bien para un estudio detallado de la prospectiva en la actividad pública se recomienda acudir a una lectura detenida de SÁNCHEZ SÁNCHEZ (2022).

<sup>10</sup> BERNSTEIN (2015).

<sup>11</sup> SÁNCHEZ MACÍAS y RODRÍGUEZ LÓPEZ (2021).

<sup>12</sup> El estudio, por tanto, de fórmulas de predicción de escenarios en el ámbito público debería basarse en la experiencia previa del sector privado, tal y como proponemos en este trabajo para la implantación de canales de denuncia eficaces y comprometidos.

<sup>13</sup> ATIENZA RODRÍGUEZ (2006).

<sup>14</sup> Así lo recoge MINSAIT (2021).

<sup>15</sup> RIVERO ORTEGA (2017).

<sup>16</sup> RIVERO ORTEGA (2022a y b).

así como analizar los casos de mayor dificultad superada para afrontar los propios problemas transformando toda esta información en conocimiento aplicado<sup>17</sup>.

La participación de los ciudadanos en la vida pública, señala VILLORIA MENDIETA<sup>18</sup>, no solo debe reducirse al proceso electoral, sino que, en cumplimiento del deber constitucional impuesto a los poderes públicos, los ciudadanos también deben estar capacitados para alertar de conductas impropias en el ejercicio de la actividad pública<sup>19</sup>.

En lo relativo a las políticas de integridad, los canales de denuncia pueden convertirse en una herramienta poderosa para recabar, de primera mano, esta información y para procesarla, gracias a la tecnología, tratando no solo de prevenir y detectar los supuestos de posible fraude sino para diseñar fórmulas o parámetros que permitan identificar situaciones de riesgo, antes incluso de que se produzcan e incorporar soluciones para prevenirlas.

La información que se obtiene de los agentes directamente vinculados con el caso concreto y de aquellos que están más cerca de los posibles conflictos es clave. Como ya se ha señalado, la integración de este conocimiento disperso en la sociedad permite identificar y ofrecer soluciones a los problemas públicos. Sin embargo, la formulación de mecanismos de denuncia de irregularidades no ha encontrado todavía en España la aceptación recibida en otros entornos jurídicos y culturales.

El último Índice de Percepción de la Corrupción (IPC) 2022 de Transparencia Internacional ha supuesto, en la percepción de los ciudadanos españoles en torno a la corrupción, la bajada de un punto en relación con el 2021. Con esta calificación, España ocupa la posición 35/180 del ranking global del IPC, junto con Botsuana, Cabo Verde y San Vicente y Las Granadinas, y se mantiene en el puesto número 14/27 de la Unión Europea, bajando dos posiciones con respecto al año 2020. De esta forma, aunque estadísticamente no es significativo, Transparencia Internacional concluye que España no progresa en la lucha contra la corrupción y que requiere una llamada a la acción a las autoridades públicas, al sector privado y a la sociedad civil<sup>20</sup>.

Por su parte, el Eurobarómetro especial sobre corrupción de 2022 de la Comisión Europea refleja que, en España, el 89 % de los encuestados considera que la corrupción está extendida en su país cuando la media de la UE es del 68 %, y el 46 % de ellos cree que la corrupción afecta personalmente a su vida diaria en contraste con el 24 % de la media europea<sup>21</sup>.

Además, los datos demuestran que la sociedad española con carácter general aún no acepta la denuncia como mecanismo de prevención y de autoprotección de las organizaciones, a diferencia de lo que ocurre en otras culturas, de lo que se podría deducir que es necesario dedicar más recursos a la difusión de las ventajas sociales que tienen los canales de denuncias de forma que se superen las reticencias culturales que tienen en España estas herramientas, en el sector privado y también en el público<sup>22</sup>.

---

<sup>17</sup> A este respecto es interesante recordar cómo la tecnología ha jugado un papel decisivo en la aplicación de este nuevo modelo de gestión pública inteligente. CRIADO GRANDE (2016) nos lo recordaba al enumerar los factores que generan este poder transformador cuando decía que “las capacidades disruptivas de las nuevas tecnologías sociales en el sector público derivan, entre otros, de factores como: 1) la incorporación de los agentes externos de la organización a los procesos de adopción de decisiones, 2) las dinámicas colaborativas que se requieren para poner en marcha determinados proyectos en grupos de trabajo distribuidos (holocracia), 3) la transparencia radical de los procesos de relación con el entorno, 4) la transformación de las dinámicas de intermediación, 5) la reducción de los costes de puesta a disposición de la información, 6) así como la evaluación continuada ligada a la trazabilidad de las acciones en esos nuevos espacios cooperativos digitales”.

<sup>18</sup> VILLORIA MENDIETA (2020).

<sup>19</sup> Esta referencia al trabajo de VILLORIA MENDIETA (2020) es esencial en materia de ética e integridad en las administraciones públicas.

<sup>20</sup> El “Índice de Percepción de la Corrupción (IPC) 2022”, de Transparencia Internacional, publicado el 31 de enero de 2023, cuenta con numerosas funcionalidades y se puede consultar en <https://www.transparency.org/en/cpi/2022>.

<sup>21</sup> El conocido como “Eurobarómetro especial sobre la corrupción” es ya una herramienta fundamental para conocer el estado de opinión de la ciudadanía de los diferentes Estados Miembros de la Unión Europea, cuenta con un portal de datos abiertos para la consulta y reutilización de los mismos y se puede consultar en <https://europa.eu/eurobarometer/surveys/detail/2658>.

<sup>22</sup> Todavía queda mucho camino que recorrer en el sector privado español. Según el “Estudio sobre la función de compliance en las empresas españolas”, elaborado por ASCOM, “el hecho de que hay un porcentaje significativo de

Los esfuerzos para prevenir la corrupción todavía se fundamentan, principalmente, en un modelo racional de toma de decisiones por lo que repensar las políticas de integridad desde la perspectiva del comportamiento humano puede ayudar a capitalizar la cultura ética y de integridad promovida desde los poderes públicos<sup>23</sup>.

Las políticas de integridad se basan a menudo en el supuesto de que las personas aprovecharán una oportunidad de conducta indebida siempre y cuando las ganancias superen el riesgo de posibles consecuencias negativas. Este planteamiento genera un refuerzo de los mecanismos de control estrictos, de las sanciones y de la limitación de la discrecionalidad de quienes toman decisiones con el consecuente riesgo de parálisis del sistema e incremento del sentimiento de desconfianza.

Sin embargo, la investigación conductual y la gestión de los entornos de riesgo e incertidumbre de forma heurística, representada en la literatura económica por STIGLITZ<sup>24</sup>, KAHNEMAN, SLOVIC y TVERSKY<sup>25</sup> o THALER y SUNSTEIN<sup>26</sup>, entre otros, cuestiona este análisis estrictamente racional de coste-beneficio e incorpora un enfoque basado en las preferencias sociales y en el conocimiento de los prejuicios del comportamiento y de las limitaciones cognitivas del ser humano. Este enfoque permite abordar, de manera mucho más realista, algunas de las críticas de las políticas anticorrupción tradicionales al tiempo que presenta un argumento para promover, en definitiva, la confianza y una cultura organizacional de integridad<sup>27</sup>.

El reto se encuentra, entonces, en comprender cómo debemos diseñar de estos canales de denuncia para que puedan cumplir, de manera eficaz, su cometido. A lo largo de las siguientes líneas encontrarán una propuesta de principios generales de aplicación que, estamos seguros, arrojarán luz a este dilema.

## II. EL NUEVO MARCO NORMATIVO PARA LOS CANALES DE DENUNCIA: DE LA DIRECTIVA EUROPEA *WHISTLEBLOWER* A LOS PLANES DE MEDIDAS ANTIFRAUDE DEL PLAN DE RECUPERACIÓN, TRANSFORMACIÓN Y RESILIENCIA

### 1. La Directiva *Whistleblower*

Como respuesta a la necesidad de reforzar los marcos de integridad y diseñar mecanismos que protejan el papel del denunciante, en el contexto europeo, fue aprobada 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*<sup>28</sup>.

---

empresas, porcentaje que aumenta aún más en las empresas de menor tamaño, que no destinan presupuesto al apoyo digital (bases de datos y aplicaciones informáticas) y a otras herramientas necesarias para ejercer de forma eficaz la función de *compliance* da una idea de que, a pesar de que sí que ha comenzado a implantarse y va avanzando poco a poco, el grado de madurez de la función de *compliance* es aún bajo con carácter general, ya que estas herramientas son esenciales hoy en día para identificar, prevenir y dar respuesta a los riesgos de *compliance*. El 100% de las empresas encuestadas cuentan con un Código Ético, pero solo el 98.5% con un canal de denuncias. Pese a que un elevado porcentaje de compañías manifiesta contar con un canal de denuncias como herramienta del sistema de gestión de Compliance, prácticamente la mitad de estas (51,9%) no ha recibido denuncias en los 12 últimos meses y el 85,7% ha recibido menos de 5 denuncias en 12 meses. Hay, sin embargo, diferencias sustanciales entre las empresas de mayor y menor tamaño, ya que en las más pequeñas estos porcentajes llegan hasta el 76,2% y el 100% y en las grandes se reducen al 32,0% y 70% respectivamente”.

<sup>23</sup> La aplicación de percepciones conductuales en la formulación de políticas públicas de todo tipo es, hoy en día, una realidad en el contexto de la OCDE, de la Unión Europea o del Banco Mundial. En concreto, debemos acudir al informe OCDE (2018), elaborado en el marco de los estudios de la OCDE sobre gobernanza pública, así como al Dictamen del Comité Económico y Social Europeo (2017) para un análisis detallado de sus propuestas.

<sup>24</sup> STIGLITZ (2002).

<sup>25</sup> KAHNEMAN, SLOVIC y TVERSKY (1982).

<sup>26</sup> THALER y SUNSTEIN (2008).

<sup>27</sup> En relación con la aplicación de incentivos basados en el conocimiento para la formulación de políticas públicas, resulta interesante consultar a CEREZO PRIETO y FRUTOS ESTEBAN (2022). Y para un análisis más exhaustivo sobre su aplicación a las políticas de integridad a DUPUY y NESET (2020).

<sup>28</sup> Puede ser consultada en <https://www.boe.es/doue/2019/305/L00017-00056.pdf>.



El objetivo principal de la Directiva es el de establecer unas normas mínimas comunes que proporcionen un elevado nivel de protección de las personas que faciliten información sobre infracciones del Derecho de la Unión en ámbitos como la contratación pública, la prevención del blanqueo de capitales y la financiación del terrorismo, la salud pública o la protección de la privacidad y de los datos personales. La enumeración de estos ámbitos de aplicación de la Directiva se entiende sin perjuicio de la posibilidad que tienen los Estados Miembros de ampliar la protección en su derecho nacional a otros ámbitos o actos no previstos en la misma.

Las disposiciones de la Directiva establecen, por un lado, la obligación de las organizaciones públicas y privadas de implementar canales de denuncia internos y externos para recibir forma veraz y segura la información remitida por los denunciantes y, por otro, reconocen un listado de medidas de protección que las mismas organizaciones deben desplegar para evitar el riesgo de represalias o para poder reaccionar cuando estas ya se han producido. Además, la norma europea impone a los Estados Miembros la función de designar autoridades nacionales que se responsabilicen del cumplimiento de estas disposiciones y garanticen la buena ejecución de las mismas incorporando una serie de obligaciones de información estadística y registro<sup>29</sup>.

Con esta protección cualificada del estatuto del denunciante se trata de compensar el desequilibrio de poder en el que pueden encontrarse las personas denunciadas frente a sus propias organizaciones, así como mitigar el riesgo de sufrir represalias laborales. Por tanto, el despliegue de las disposiciones contenidas en la Directiva exige la existencia de una relación estrecha entre la denuncia y el trato desfavorable sufrido, directa o indirectamente, materializado en actos u omisiones producidas en un contexto laboral y causantes de perjuicios.

Las organizaciones obligadas al establecimiento de estos canales de denuncia son todas las entidades jurídicas del sector privado y del sector público, incluidas las entidades que sean propiedad o estén sujetas al control las mismas, con la única excepción de aquellas que no empleen a más de 50 trabajadores o los municipios de menos de 10.000 habitantes que podrán utilizar, para dar por cumplidas sus obligaciones, los canales de denuncia externos establecidos por la autoridad nacional<sup>30</sup>.

El concepto de denunciante es particularmente amplio en esta Directiva al abarcar tanto a trabajadores, trabajadores no asalariados, accionistas y personas con poder de administración y dirección, voluntarios, trabajadores en prácticas, proveedores, contratistas o subcontratistas y

---

<sup>29</sup> La obligación de crear esta figura es especialmente relevante así, y en relación con la designación de autoridades nacionales responsables de la recepción y seguimiento de las denuncias que podrán ser autoridades judiciales, organismos de regulación o de supervisión competentes en los ámbitos específicos de que se trate, o autoridades con una competencia más general a escala central dentro de un Estado miembro, autoridades encargadas del cumplimiento del Derecho, organismos de lucha contra la corrupción o defensores del pueblo, el considerando 65 dispone: “Como destinatarias de las denuncias, las autoridades a las que se designe como competentes deben tener las capacidades y competencias necesarias para garantizar un seguimiento adecuado, también para valorar la exactitud de las alegaciones formuladas en la denuncia y para ocuparse de las infracciones denunciadas, a través de la apertura de una investigación interna, de una investigación, del enjuiciamiento, de una acción de recuperación de fondos u otras medidas correctoras adecuadas, de conformidad con su mandato. Alternativamente, dichas autoridades deben tener las competencias necesarias para remitir la denuncia a otra autoridad que deba investigar la infracción denunciada, y garantizar que haya un seguimiento adecuado por parte de dicha autoridad. En particular, cuando los Estados miembros deseen establecer canales de denuncia externa a nivel central, por ejemplo, en el ámbito de las ayudas otorgadas por los Estados, los Estados miembros deben establecer las salvaguardias adecuadas para garantizar el respeto de los requisitos de independencia y autonomía establecidos en la presente Directiva. El establecimiento de dichos canales de denuncia externa no debe afectar a las competencias de los Estados miembros o de la Comisión en materia de supervisión en el ámbito de las ayudas estatales, ni tampoco debe afectar a la competencia exclusiva de la Comisión en lo que respecta a la declaración de compatibilidad de dichas ayudas, en particular con arreglo al artículo 107, apartado 3, del Tratado de Funcionamiento de la Unión Europea (TFUE). Por lo que se refiere a las infracciones de los artículos 101 y 102 del TFUE, los Estados miembros deben designar como autoridades competentes a las mencionadas en el artículo 35 del Reglamento (CE) n.º 1/2003 del Consejo (35), sin perjuicio de las competencias de la Comisión en este ámbito”.

<sup>30</sup> No obstante, los Estados Miembros pueden establecer la inaplicación de estas excepciones, estableciendo requisitos menos exigentes, cuando o bien estén obligadas a establecerlos en virtud de otras disposiciones del derecho de la Unión o se haya realizado una adecuada evaluación de riesgo y así se determine.

cualquier persona que trabaje bajo el mando de estos como a extrabajadores y personas que se encuentran en un proceso de selección y contratación, facilitadores y terceros vinculados.

Las denuncias pueden presentarse por diferentes vías<sup>31</sup>, y todas ellas deberán garantizar la confidencialidad del denunciante, que no verá revelada su identidad sin su consentimiento expreso salvo que constituya una obligación necesaria y proporcionada en el contexto de una investigación judicial y con el objetivo de salvaguardar el derecho de defensa de personas afectadas. La protección de la identidad del denunciante será también de aplicación a las personas afectadas, en garantía de su derecho a la tutela judicial efectiva y a la presunción de inocencia.

En relación con el anonimato, la Directiva otorga a los Estados Miembros la facultad de exigir o no a las entidades jurídicas afectadas y a las autoridades competentes la admisibilidad de las denuncias presentadas de forma anónima.

La Directiva prioriza el uso de los canales de denuncia internos sobre la base de que, de esta manera, se contribuye a fomentar una cultura de buena comunicación y responsabilidad social empresarial en las organizaciones en la que los denunciantes contribuyen de manera significativa a la autocorrección y la excelencia dentro de la organización.

No obstante, conscientes de que la falta de confianza en la eficacia de las denuncias es uno de los principales factores que desalientan a los denunciantes potenciales, obliga también a las autoridades competentes al establecimiento de canales de denuncia externos adecuados, a que sigan con diligencia las denuncias recibidas y, en un plazo razonable, den respuesta a los denunciantes.

Tanto en el caso de canales internos como externos, sus responsables deben llevar un registro de las denuncias recibidas, cumpliendo los requisitos de confidencialidad exigidos por las disposiciones en materia de protección de datos, así como remitir información al denunciante sobre el estado de la denuncia, las medidas y acciones adoptadas y su justificación en unos plazos determinados por la misma norma<sup>32</sup>.

Dentro de las medidas de protección del denunciante se encuentran todas las que sean necesarias para prohibir las represalias, su amenaza y tentativas y otras medidas de apoyo como la información y asesoramiento gratuito sobre procedimientos y recursos disponibles, y la asistencia jurídica, financiera o psicológica.

En concreto, podrán beneficiarse de esta protección los denunciantes que tengan motivos razonables para pensar que la información sobre infracciones denunciadas es veraz en el momento de la denuncia y que hayan denunciado por canales, internos o externos o hayan hecho una revelación pública<sup>33</sup>.

Además, con la finalidad de garantizar la efectividad del régimen de protección recogido en la Directiva, los Estados Miembros están obligados a publicar en sus páginas web toda la información relativa a los canales de denuncia, establecer un régimen de sanciones efectivas, disuasorias y proporcionadas, revisar los procedimientos periódicamente y enviar a la Comisión Europea la información pertinente relativa a la ejecución y aplicación de la misma.

## 2. La Ley española de protección del informante

---

<sup>31</sup> El considerando 53 de la Directiva establece: “más concretamente, los canales de denuncia deben permitir que las personas denuncien por escrito y que lo puedan hacer por correo, a través de un buzón físico destinado a recoger denuncias o a través de una plataforma en línea, ya sea en la intranet o en internet, o que denuncien verbalmente, por línea de atención telefónica o a través de otro sistema de mensajería vocal, o ambos. A petición del denunciante, dichos canales deben también permitir denunciar mediante la celebración de reuniones presenciales en un plazo razonable”.

<sup>32</sup> El Considerando 58 dispone: “un plazo razonable para informar al denunciante no debe exceder de tres meses. Cuando todavía se esté considerando el seguimiento apropiado, el denunciante debe ser informado de ello, así como de cualquier otra respuesta que haya de esperar”.

<sup>33</sup> La Directiva define “revelación pública” como aquella que se produce cuando el denunciante que ha utilizado los canales previstos sin que se produzca una respuesta apropiada pero tiene motivos suficientes para pensar que la infracción puede suponer un peligro inminente y manifiesto para el interés público o que la autoridad nacional no sea capaz de dar un tratamiento efectivo a la infracción por razones de connivencia o riesgo de destrucción de pruebas.

El 23 de septiembre de 2022 fue publicada en el Boletín Oficial de las Cortes Generales la configuración definitiva del proyecto 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, comenzando de esta manera su tramitación parlamentaria.

La redacción finalmente aprobada, en numerosos aspectos mejorada respecto de su primera versión, ha sido sancionada por el Rey y publicada en el Boletín Oficial del Estado el 21 de febrero de 2023<sup>34</sup>. La entrada en vigor prevista en la Disposición final duodécima recoge la clásica *vacatio legis* de 20 días desde su publicación, si bien, debemos destacar la aplicación progresiva y sin demasiado orden de sus obligaciones<sup>35</sup>.

La norma de protección del informante debería haberse transpuesto a nuestro ordenamiento jurídico antes del 17 de diciembre de 2021 por lo que la primera consideración que debemos realizar es el evidente retraso de nuestro país en el cumplimiento de sus obligaciones con las instituciones europeas lo que ha dado lugar, en enero de 2022, a la incoación de un procedimiento de infracción contra el Reino de España, aunque, en principio, sin consecuencias sancionadoras.

El proceso de elaboración y aprobación de la norma ha estado sometido al examen de numerosos organismos de lucha contra la corrupción y a la fiscalización de las organizaciones de la sociedad civil en defensa de la transparencia y de la cultura del cumplimiento normativo lo que se ha traducido en relevantes aportaciones y mejoras, así como en las denuncias de los aspectos injustificables del proyecto español<sup>36</sup>.

La finalidad de la ley española no es otra que otorgar una protección adecuada frente a represalias a las personas físicas que utilizando los procedimientos previstos en la norma informen de las acciones u omisiones incluidas en su ámbito material de aplicación. Aunque en el curso de la negociación de la ley se incorporó, desde mi punto de vista de manera muy acertada, una segunda finalidad “el fortalecimiento de la cultura de la información, de las infraestructuras de integridad de las organizaciones y el fomento de la cultura de la información o comunicación como mecanismo para prevenir y detectar amenazas al interés público”.

Una de las primeras características de la ley española que nos llaman la atención es el apartamiento en el uso de las clásicas denominaciones “denunciante y canal interno y externo de denuncias” de la Directiva europea que se ven sustituidas por los términos “informante, sistemas internos de información, canales internos de comunicación y canal externo de comunicaciones” a lo largo de todo su articulado. La elección de esta terminología podría derivar de la necesidad de diferenciar estos mecanismos particulares de comunicación impulsados por la normativa europea

---

<sup>34</sup> Se puede consultar en <https://www.boe.es/buscar/pdf/2023/BOE-A-2023-4513-consolidado.pdf>.

<sup>35</sup> El plazo máximo para el establecimiento de sistemas internos de información o adaptación de los existentes para Administraciones, organismos y empresas se extiende hasta el 13 de junio de 2023, pero para aquellas entidades del sector privado de menos de 249 trabajadores y municipios de menos de diez mil habitantes será el 1 de diciembre de 2023.

Castilla y León ha publicado, en su Boletín Oficial de 15 de mayo de 2023, el Decreto-ley 3/2023, de 11 de mayo, por el que se regula el Sistema Interno de Información de la Administración de la Comunidad de Castilla y León [<https://www.boe.es/buscar/pdf/2023/BOCL-b-2023-90202-consolidado.pdf>] para cumplir con sus obligaciones de adaptación a la normativa indicada. La adaptación de los canales y procedimientos de información externa existentes se deberá producir antes del 13 de septiembre de 2023, pero hasta el 13 de marzo de 2024 podrá aprobarse el real decreto que regule el Estatuto de la Autoridad Independiente de Protección del Informante. Esta autoridad podrá firmar convenios con las Comunidades Autónomas para actuar como órgano externo de comunicaciones si no se opta por crear una autoridad independiente autonómica. El 13 de septiembre de 2024 es la fecha que se marca el Gobierno para aprobar una Estrategia de Lucha contra la corrupción fruto de una evaluación del cumplimiento de los objetivos y con propuestas de mejora para paliar sus deficiencias.

<sup>36</sup> La norma española ha sido duramente criticada por la *Whistleblowing International Network* (WIN) en una misiva enviada a la Comisión Europea, justo antes del trámite de votación de enmiendas en el Senado, en la que podemos encontrar nueve aspectos de necesaria consideración para su adecuación a los criterios y al espíritu de la Directiva. Su texto completo se puede consultar en <https://es.scribd.com/document/624367047/25-01-23-WIN-Letter-EC-Re-Spain-Transposition-fin#>.



de la institución jurídica de la denuncia y de la obligación de denunciar, que únicamente se genera, en nuestro ordenamiento jurídico, en los supuestos y con los requisitos recogidos en la Ley de Enjuiciamiento Criminal<sup>37</sup>, como señala LEÓN ALAPONT, o en el intento de prestigiar la figura del clásico denunciante con un uso del lenguaje más neutro, como apunta JIMÉNEZ FRANCO<sup>38</sup>.

La norma española ha sido duramente criticada al circunscribir su ámbito material de aplicación únicamente a las comunicaciones de conductas —penales y administrativas, graves o muy graves—, vulnerando, como poco, el espíritu de la Directiva comunitaria a pesar de que su Exposición de Motivos establezca que “la generalización de un Sistema Interno de Informaciones facilitará la erradicación de cualquier sospecha de nepotismo, clientelismo, derroche de fondos públicos, financiación irregular u otras prácticas corruptas”, como resalta JIMÉNEZ FRANCO<sup>39</sup>; luego no lo afronta en su articulado.

Si se pretende incentivar una verdadera cultura de integridad, la protección debería ampliarse a las malas prácticas, tanto administrativas como privadas, como pueden ser los abusos de autoridad, la mala gestión, las conductas discriminatorias o contrarias o lesivas al interés general, especialmente cuando el artículo 7.4, que regula el canal interno de información, prevé que estos estén habilitados para recibir este tipo de comunicaciones pero recordando que quedarán fuera del ámbito de protección dispensado por la norma. En concreto, la información comunicada que despliega los instrumentos de protección de la norma comprende la referida a acciones u omisiones que puedan constituir infracciones del Derecho de la Unión Europea de las contenidas en el Anexo de la Directiva, que afecten a los intereses financieros de la Unión Europea o incidan en el mercado interior así como la referida a aquellas acciones u omisiones que puedan ser constitutivas de infracción penal o administrativa grave o muy grave, entendiéndose comprendidas todas las que impliquen quebranto económico para la Hacienda Pública y para la Seguridad Social. Referencia confusa e insuficiente, contraria a los principios que deben inspirar un *compliance* integral.

La protección prevista en la norma, además, tiene límites y no alcanza a las informaciones que afecten a la información clasificada, a los procedimientos de contratación que contengan este tipo de información o hayan sido declarados secretos, al secreto profesional de los profesionales de la medicina y abogacía, al deber de confidencialidad de Fuerzas y Cuerpos de Seguridad ni a las deliberaciones judiciales.

Esta redacción del ámbito material de la norma en términos así de imprecisos generará problemas de interpretación jurídica que, en última instancia, exigirán un estudio previo de comprobación de la tipicidad del hecho denunciado por parte del personal que deberá estar especialmente cualificado, que conducirán a la admisibilidad o no de la denuncia presentada con el consiguiente retraso en su tramitación y desincentivarán, fruto de la indeterminación, la comunicación de estas conductas por parte de los particulares.

Del mismo modo, se prevé la obligación de traslado a la Autoridad Independiente de Protección del Informante de aquellas comunicaciones que reciban otras autoridades que no sean competentes para investigar el supuesto concreto, generando los mismos problemas de interpretación y competencia señalados.

---

<sup>37</sup> LEÓN ALAPONT (2022), quien en línea con el informe del Consejo General del Poder Judicial sobre el Anteproyecto de 26 de mayo de 2022, señala que “... 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”, en consonancia con lo apuntado por FERNÁNDEZ AJENJO (2022), cuando recuerda que el deber jurídico de denunciar se impone por los ordenamientos con sumo cuidado y bastantes excepciones.

<sup>38</sup> JIMÉNEZ FRANCO (2023), quien incorpora la siguiente reflexión: “Lo más difícil, por ende, es la consecución de un cambio de paradigma en la concepción ética de la figura del informante, que actúa teniendo presente la defensa del interés general y la búsqueda del bien común, y tratarlo más como un «valiente», un «héroe» o una persona con una actitud cívica encomiable, como ocurre en la tradición anglosajona, donde el «whistleblower» es alabado y respetado. En este sentido, el término «informante» es más neutro”.

<sup>39</sup> JIMÉNEZ FRANCO (2023).

En lo relativo a las entidades obligadas a establecer estos sistemas internos de información, que abarcan tanto el canal, el responsable del sistema como el procedimiento, también la norma española se caracteriza por su amplitud ya que será de aplicación a todas las personas físicas y jurídicas de naturaleza privada siempre que tengan contratadas a 50 o más trabajadores y a todas las entidades que integran el sector público.

No se acoge, por tanto, a las excepciones que la Directiva comunitaria permite para los Ayuntamientos de menos de 10.000 habitantes aun cuando para estos se prevé la posibilidad de compartir medios para la recepción de informaciones con otras administraciones que ejerzan sus competencias en la misma Comunidad Autónoma siempre que puedan garantizar la independencia del sistema de gestión y que los canales aparezcan diferenciados entre sí lo que en la práctica significa que cuenten con un responsable propio del sistema interno. Misma posibilidad que ofrece a las entidades con personalidad jurídica propia, adscritas a una administración territorial y de menos de 50 trabajadores.

Del mismo modo y atendiendo a las posibles cargas de gestión que esto puede suponer para las administraciones más modestas se permite la externalización de la gestión material del canal siempre que se acredite insuficiencia de medios propios para realizar esta función, ofrezca con todas las garantías adecuadas y el control de la gestión del sistema se residencie siempre en el ámbito interno de la organización, sin que pueda implicar ejercicio de potestades públicas y/o funciones reservadas a personal funcionario de carrera<sup>40</sup>.

De forma expresa y con independencia del número de empleados obliga a contar con un sistema interno de información a todos los partidos políticos, sindicatos, organizaciones empresariales, así como a las fundaciones creadas por unos y otros, siempre que reciban o gestionen fondos públicos, los órganos constitucionales, los de relevancia constitucional e instituciones autonómicas análogas a los anteriores<sup>41</sup>.

En el supuesto de las entidades del sector privado se mantiene el límite de los 50 trabajadores de la Directiva, aunque las organizaciones que cuenten entre 50 y 249 trabajadores pueden compartir medios. Resulta especialmente significativo, en el caso español en el que las empresas con menos de 50 trabajadores representan el 99,3% del total y el 72% del empleo, frente a la UE donde representan de media el 65% y donde la mayor parte de su tejido productivo está compuesto por pymes y micro pymes<sup>42</sup>, que la obligación de contar con un sistema interno de información no alcance a las empresas de menos de 50 trabajadores por lo que, entendemos, todas las denuncias de irregularidades detectadas en estos entornos deberán canalizarse a través de la Autoridad Independiente de Protección del Informante y su canal externo de comunicaciones.

Son sujetos considerados susceptibles de protección las personas físicas informantes que trabajen en el sector privado o público y que hayan obtenido información sobre infracciones en un contexto laboral o profesional de forma similar a lo establecido en la norma europea<sup>43</sup>.

La adecuada conceptualización de la figura del denunciante, típicamente anglosajona, en la transposición española, es esencial para no comprometer la eficacia ni colisionar con otras

---

<sup>40</sup> Se considera gestión del sistema únicamente la recepción de informaciones, como reconoce expresamente el artículo 6.1 de la norma, excluyendo de estas tareas, por ejemplo, las de investigación de la denuncia o comunicación.

<sup>41</sup> En la redacción inicial del Anteproyecto de Ley se refería expresamente a “la Casa de Su Majestad el Rey, a los órganos constitucionales e instituciones autonómicas análogas creadas por los correspondientes Estatutos de Autonomía”, redacción ahora sustituida por una más general.

<sup>42</sup> La Definición de PYME está recogida en el Anexo I del Reglamento (UE) n.º 651/2014 de la Comisión en el que definen los tipos de empresa y se fija un método transparente para calcular los límites financieros (no superar una cifra de volumen de negocio o de balance general) y el número de empleados.

<sup>43</sup> Con el mismo espíritu que la Directiva Europea, el concepto de “trabajador” se extiende a aquellas personas cuya relación laboral ha finalizado o que aún no ha comenzado pero conocen los hechos en el marco de esta relación pasada o futura. También se extenderá la protección a terceros relacionados con el informante en los términos expresados en su artículo 3.

instituciones próximas que ya forman parte de nuestro sistema jurídico como nos recuerda GARCÍA MORENO<sup>44</sup>.

Sin embargo, como hemos podido comprobar, la norma española no se ha decidido a extender el concepto de informante a aquellas otras personas, físicas o jurídicas, que pueden facilitar información veraz, aunque no se encuentren vinculadas de forma laboral o profesional a la organización ni tampoco ha recogido medidas de lenidad o recompensa a favor de los informantes como ocurre en otros ordenamientos jurídicos. Algunos autores como SENDÍN GARCÍA<sup>45</sup> o JIMÉNEZ FRANCO<sup>46</sup> consideran un error no haber atribuido al informante la consideración de interesado en estos procedimientos y lo consideran una grave contradicción con elementos estructurales de un Estado democrático<sup>47</sup>.

Una vez analizado el ámbito material y personal de aplicación de la norma de protección del denunciante así como las entidades obligadas a disponer de un sistema interno de información, debemos desgranar los tres procedimientos de comunicación de infracciones que la Ley considera válidos para desplegar su protección: en primer lugar y de forma preferente a través de los sistemas internos de información o, en cualquier caso, a través del canal externo de comunicaciones que gestiona la Autoridad Independiente de Protección del Informante y, por último, en forma de relevación pública siempre que respeten una serie de condiciones.

En primer lugar, reconoce que los sistemas internos de información son el cauce preferente para comunicar las infracciones contenidas en su articulado. Estos sistemas pueden integrar varios canales internos de comunicación existentes en una misma organización y deben ser implementados por el órgano de administración o de gobierno de la persona jurídica, previa consulta a los trabajadores.

Entre otras características definidas de forma general en la norma, los sistemas internos de información deben estar diseñados y gestionados de forma segura, ser independientes y aparecer diferenciados de otros sistemas, garantizar el tratamiento confidencial de la identidad del informante, de terceros y de todo el proceso, deben contar con un responsable encargado del procedimiento de gestión de las comunicaciones presentadas verbal y/o por escrito, recoger la política de integridad dándole la suficiente publicidad y establecer las garantías de protección con que cuentan los informantes.

El responsable del sistema, como encargado del procedimiento de gestión de las comunicaciones, es decir, de la recepción de las informaciones y la tramitación de los expedientes de investigación, debe garantizar su tramitación diligente y la observancia de un contenido mínimo y principios como, por ejemplo, identificar los canales internos disponibles e incluir información clara sobre los canales externos de información existentes<sup>48</sup>.

En el caso del sector privado, será un alto directivo nombrado por el órgano de administración que desarrollará de forma independiente y autónoma sus funciones, pudiendo recaer en la persona que ejerza las funciones de *Compliance Officer* o “en otra persona que ejerza otras funciones siempre que se trate de evitar posibles situaciones de conflicto de interés” expresión que, a nuestro juicio, no resulta suficientemente garantista. En el ámbito del sector público, compartimos la recomendación de la Agencia Valenciana Antifraude que anima a todas las entidades a designar un responsable de integridad que asuma las funciones vinculadas a los canales internos de información,

---

<sup>44</sup> Para profundizar sobre los orígenes y el concepto de informante podemos acudir a los numerosos estudios de la autora y, en concreto, a su trabajo de 2021.

<sup>45</sup> SENDÍN GARCÍA (2019).

<sup>46</sup> JIMÉNEZ FRANCO (2023).

<sup>47</sup> Para conocer con mayor profundidad esta cuestión se puede acudir a SENDÍN GARCÍA (2019).

<sup>48</sup> Las administraciones públicas que ya cuentan con un sistema interno de información están atribuyendo a la Inspección de Servicios las tareas de responsable del sistema pero, difícilmente, podrá cumplir algunas de las funciones atribuidas, por ejemplo la de ofrecer información sobre los canales externos existentes, cuando la Ley concede al Gobierno un plazo mayor para su creación, lo que puede generar no solo problemas de aplicación temporal sino de responsabilidad del encargado del sistema (véase el sistema interno de información de la Administración de Castilla y León o del Ministerio de Universidades).

pero también todas aquellas que requiera la ejecución del plan de integridad institucional y/o de cada uno de los marcos de integridad que impone la vigente legislación en materia de transparencia y buen gobierno, tales como: códigos éticos, procedimientos de prevención y control de los conflictos de interés, formación, etcétera<sup>49</sup>.

El anonimato versus la confidencialidad en este tipo de instrumentos ha sido siempre una cuestión polémica en la que encontramos posturas doctrinales contrapuestas<sup>50</sup>. La ley, a lo largo de su articulado, se preocupa por proteger el tratamiento confidencial de la identidad de los sujetos implicados y de la información surgida a lo largo del proceso y bajo esta condición reconoce determinados derechos y obligaciones. Sin embargo, con carácter adicional, establece la posibilidad de permitir el anonimato en las comunicaciones cuando describe sucintamente los canales internos de información que se integran en los sistemas internos y cuando se refiere a la recepción de las comunicaciones por el canal externo al indicar que “las comunicaciones pueden llevarse a cabo de forma anónima”.

Consideramos oportuno advertir que, en los supuestos del uso del anonimato, los derechos de información y seguimiento del procedimiento que se prevén en la norma e incluso la protección especial recogida en su Título VII no serán de aplicación si los informantes no se identifican posteriormente lo que no parecería generar los incentivos suficientes para el uso de esta posibilidad que, desde mi punto de vista, se concibe en cualquier caso como una vía residual<sup>51</sup>.

El tratamiento de los datos de carácter personal que puedan realizar los responsables de los sistemas es un asunto especialmente delicado. De forma preventiva y para garantizar la efectividad de los canales, declara lícito el tratamiento de los datos personales generados en todo el procedimiento de gestión de las comunicaciones, incluso en caso de oposición manifestada por el denunciado<sup>52</sup>.

En segundo lugar, en cumplimiento de las disposiciones europeas y como cauce válido de comunicación de las infracciones, se prevé la existencia de un canal externo de información gestionado por la Autoridad Independiente de Protección del Informante o a través de las autoridades u órganos autonómicos correspondientes. Cualquier persona física puede acudir, ya sea directamente o previa comunicación a través del correspondiente canal interno, al canal externo de información. Una vez presentada la información se registrará en el sistema de gestión de información, contenido en una base de datos segura y de acceso restringido, cumplimentando una serie de datos estandarizados y dando cuenta al informante en un plazo no superior a cinco días.

La ley autoriza la creación de una autoridad administrativa independiente, como ente de derecho público con personalidad jurídica propia y plena capacidad, dotado de autonomía e independencia orgánica y funcional respecto del Gobierno y del sector público, así como de toda entidad cuya actividad pueda ser sometida a su supervisión y concede el plazo de un año desde su entrada en vigor para la aprobación de su Estatuto. El previsible impacto que este desarrollo normativo generará en la gestión de los canales de denuncia y, por tanto, en la protección de los informantes

---

<sup>49</sup> A favor de que el mismo *Compliance Officer* sea el responsable de la supervisión del canal de denuncias están algunos autores como VEIGA MAREQUE y FERNÁNDEZ DE AVILÉS (2019).

<sup>50</sup> Diferentes autores se han pronunciado sobre la cuestión. Así, GALÁN MUÑOZ (2019) se muestra absolutamente contrario a la posibilidad del uso del anonimato, o GIMENO BEVIÁ (2021) en el que resalta sus riesgos. A favor del anonimato también encontramos a otros autores como ARÁNGUEZ SÁNCHEZ (2020), y de la vía mixta a LEÓN ALAPONT (2023), entre otros.

<sup>51</sup> En concreto, el artículo 35.3 del texto normativo referido a las condiciones de protección al reconocer 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”.

<sup>52</sup> En otro caso, debería solicitarse consentimiento expreso e individualizado al afectado en cada uno de los trámites por imperativo del Reglamento General de Protección de Datos europeo lo que, de facto, haría inoperativa la gestión ágil de las comunicaciones y el cumplimiento de los plazos exigidos en la norma.



resulta contradictorio con el régimen transitorio previsto en la propia norma que lo posterga hasta marzo de 2024<sup>53</sup>.

Las principales funciones que se le atribuyen, además de la llevanza de este canal y la adopción de las medidas de protección del informante, informar anteproyectos y proyectos de disposiciones generales, así como la competencia sancionadora en el ámbito de sus competencias y el fomento de la cultura de la información.

En su función de responsable del canal externo de comunicaciones le corresponde la recepción de las informaciones, su admisión, inadmisión o remisión en su caso al competente, la instrucción del procedimiento y su terminación con un informe y la adopción de alguna de las cuatro decisiones permitidas, a saber, archivo; remisión al Ministerio Fiscal; traslado a la autoridad competente o inicio de procedimiento sancionador. En cada una de las fases del procedimiento se debe documentar y registrar todo lo actuado e informar al informante, que haya comunicado su identidad, de los avances realizados.

La redacción finalmente aprobada de la ley compatibiliza la existencia de esta autoridad nacional con la de otras autoridades autonómicas con competencia para gestionar tanto las informaciones sobre infracciones que sean cometidas en el ámbito de las entidades del sector público autonómico y local del territorio de la correspondiente Comunidad Autónoma, como a las relativas a incumplimientos imputables a entidades del sector privado que produzcan efectos únicamente en el territorio de dicha Comunidad Autónoma. La existencia de múltiples autoridades con competencias en la materia exigirá, sin duda, profundos análisis previos de competencia para determinar la autoridad responsable con el consiguiente retraso en la tramitación de los procedimientos de investigación y rigurosos mecanismos de coordinación y cooperación, más allá de las reuniones semestrales previstas en la norma<sup>54</sup>.

Por último, se generará la protección prevista en la norma en los supuestos en los que la información se haya puesto a disposición del público pero el informante haya acudido con carácter previo a canales internos o externos sin que se hayan tomado medidas apropiadas al respecto o tenga motivos razonables para pensar que la infracción puede constituir un peligro inminente o manifiesto para el interés público o, debido a las circunstancias particulares del caso, exista un elevado riesgo de represalias y de ineficacia de la comunicación efectuada a través del canal externo, salvo que se base en el ejercicio de la libertad de expresión y de información veraz previstas constitucionalmente.

Las medidas de protección y apoyo previstas están redactadas de forma especialmente ambigua y cuentan con limitaciones que, a nuestro juicio, hacen peligrar su efectividad: La primera medida de protección que se reconoce para todos los informantes es la prohibición expresa de los actos constitutivos de represalia, su amenaza o tentativa pero siempre que se produzcan durante el procedimiento de investigación o durante los dos años siguientes a su finalización. Los actos administrativos calificados como represalias o que traten de impedir las comunicaciones serán nulos de pleno derecho y darán lugar a responsabilidad administrativa o disciplinaria, siempre en el

---

<sup>53</sup> El Proyecto de Ley presentado a las Cortes Generales sufrió importantes modificaciones en este punto. Inicialmente, como marca la Directiva Europea, se preveía la existencia de una única Autoridad Independiente con competencias en materia de protección del informante responsable de la gestión de un solo canal externo de información. Debemos esperar al desarrollo reglamentario de la figura de la AAI para comprender el verdadero funcionamiento de la agencia nacional, su relación con las autonómicas, su composición, el procedimiento de toma de decisiones, la garantía de independencia o cómo se articulará el régimen sancionador frente a las personas jurídicas públicas o los órganos constitucionales como la Casa del Rey.

<sup>54</sup> Con el mismo sentido crítico, LEÓN ALAPONT (2019) ha señalado que hubiera sido preferible para determinar la competencia entre posibles agencias territoriales optar por alguno de estos otros criterios: (i) Sujeto denunciado (persona física o jurídica). (ii) Naturaleza jurídica (empresa, partido político, sindicato, fundación). (iii) Materias. (iv) Clase de «irregularidad» denunciada. (v) Entidad de la conducta reportada. (vi) Grado de afectación, impacto, repercusión y no por el criterio territorial de la infracción. En todo caso, ante la ausencia de agencia autonómica, las Comunidades Autónomas deben suscribir con la autoridad nacional el oportuno convenio para la tramitación de las informaciones de su competencia ya que su competencia no opera por defecto, lo que resulta de nuevo una anomalía.

ámbito público sin pronunciarse sobre qué ocurre en el caso de que dichas represalias se produzcan en el contexto de una organización del sector privado.

No dará lugar a responsabilidad para el informante la revelación de información restringida salvo que los hechos sean constitutivos de delito o estén castigados por la normativa laboral o de derecho de la competencia lo que amplía notablemente la excepción de la medida de protección.

Se reconocen como medidas de apoyo de la Autoridad Independiente de Protección del Informante, aunque no se especifica de qué manera se garantiza su prestación, la información y el asesoramiento integral, accesible y gratuito, la asistencia efectiva y el apoyo financiero y, excepcionalmente, psicológico además de la asistencia jurídica gratuita que, en su caso, pudiera corresponder en los procedimientos judiciales que se inicien. De nuevo, habrá que esperar a su desarrollo normativo y a la dotación presupuestaria para poder garantizar los derechos que la norma reconoce al informante.

Por último, de forma muy positiva dentro de las medidas de protección y apoyo, se introducen incentivos clásicos de la política de clemencia, en el ámbito administrativo, para incentivar la comunicación temprana de las irregularidades y el denunciado mantiene, como no puede ser de otra manera, el derecho a la presunción de inocencia, el derecho de defensa, el de acceso al expediente y la garantía de confidencialidad de su identidad, hechos y datos del procedimiento.

Tanto para el caso de sistemas internos de información como para los canales externos de comunicación el proyecto de ley español reproduce las obligaciones europeas de publicidad y difusión de estos mecanismos, que deberán ser accesibles y fácilmente identificables<sup>55</sup> así como de registro de las comunicaciones, de las informaciones recibidas y las investigaciones realizadas.

### **3. Los planes de medidas antifraude del Plan de Recuperación, Transformación y Resiliencia**

A pesar del retraso experimentado en la transposición de la Directiva Europea al ordenamiento español y de las dificultades para la directa aplicación de la protección cualificada que acabamos de señalar, la llegada masiva a nuestro país de fondos *Next Generation EU* puede convertirse en un poderoso incentivo para la implantación definitiva de los canales de denuncia en el ámbito público.

El 21 de junio de 2020 el Consejo Europeo aprobó la creación del programa *Next Generation EU* (o Instrumento Europeo de Recuperación) como “el mayor instrumento de estímulo económico jamás financiado por la Unión Europea, en respuesta a la crisis sin precedentes causada por el coronavirus”.

El 10 de noviembre del mismo año, el Parlamento Europeo y el Consejo alcanzaron el acuerdo sobre el paquete que incluye los fondos de *Next Generation EU* y el Marco Financiero Plurianual 2021-2027 creando, en el seno de esta iniciativa, el Mecanismo Europeo de Recuperación y Resiliencia (en adelante MRR) como instrumento que pone a disposición de los 27 Estados miembros un total de 672.500 millones de euros con el objetivo de incrementar las inversiones públicas y acometer reformas que contribuyan a la recuperación de la economía, el empleo y aborden los principales retos económicos y sociales post covid-19.

---

<sup>55</sup> Expresamente dispone que “para, las autoridades competentes a las que se refiere el artículo 24 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”.

El MRR es un instrumento basado en resultados que desembolsa fondos en función de la consecución de los hitos y objetivos establecidos para las Reformas e Inversiones definidas en los Planes de Recuperación, Transformación y Resiliencia que cada Estado Miembro elabora, somete a evaluación de la Comisión Europea para su aprobación por una decisión de ejecución del Consejo y aprueba<sup>56</sup>.

España, en abril de 2021 aprobó su Plan Recuperación, Transformación y Resiliencia (en adelante PRTR) con el que se ha comprometido a cumplir una detallada agenda de inversiones y reformas y ha especificado una serie de metas, objetivos e indicadores para su seguimiento y control, como condición necesaria para la percepción de los fondos europeos<sup>57</sup>.

Los cuatro ejes transversales a través de los que se distribuyen los fondos de este instrumento europeo de gestión directa, que en España ascienden a un total de 140.000 millones de euros entre transferencias y préstamos, se proyectan en 10 políticas palanca que recogen, a su vez, los treinta componentes o líneas de acción que articulan los proyectos de inversiones y reformas regulatorias para modernizar el país.

Su objetivo es el de impulsar la recuperación económica a corto plazo y apoyar un proceso de transformación que aumente la productividad y el crecimiento potencial de la economía española en el futuro. En concreto, la política palanca IV “Una administración para el Siglo XXI” prevé la modernización y transformación de las Administraciones Públicas sobre la idea de que una prestación eficiente de los servicios públicos y su potencial tractor sobre la transformación del tejido productivo supone un factor fundamental de productividad, crecimiento y bienestar<sup>58</sup>.

El PRTR diseñado por el Gobierno de España se alinea además con la hoja de ruta de reformas recogida en la Agenda del Cambio presentada en febrero de 2019, así como con la Agenda 2030 y los Objetivos de Desarrollo Sostenible de la ONU en los que la lucha contra la corrupción de los Estados tiene un lugar prioritario.

El PRTR se refiere expresamente a la necesidad de contar con medidas para prevenir, detectar y corregir la corrupción, el fraude y los conflictos de intereses en la utilización de los fondos, para evitar la doble financiación, así como para controlar la existencia de mecanismos claros de comunicación de sospechas de fraude y prevé la creación de un canal específico de denuncias gestionado por el Servicio Nacional de Coordinación Antifraude adaptado, teóricamente, a la Directiva de protección de denunciantes.

En la práctica y hasta el momento, las administraciones públicas autonómicas y locales con Agencias u Oficinas Antifraude que garanticen la disponibilidad de mecanismos de comunicación de comportamientos contrarios a la ética en funcionamiento son minoritarias, sin embargo, es fácil prever que ahora sí, de aquí a 2027, experimentaremos considerables avances en la materia<sup>59</sup>.

---

<sup>56</sup> El Reglamento (UE) 2021/241 del Parlamento Europeo y del Consejo, de 12 de febrero de 2021, *por el que se establece el Mecanismo de Recuperación y Resiliencia*, se puede consultar en <https://www.boe.es/doue/2021/057/L00017-00075.pdf>.

<sup>57</sup> El PRTR se puede consultar en [https://www.lamoncloa.gob.es/temas/fondos-recuperacion/Documents/160621-Plan\\_Recuperacion\\_Transformacion\\_Resiliencia.pdf](https://www.lamoncloa.gob.es/temas/fondos-recuperacion/Documents/160621-Plan_Recuperacion_Transformacion_Resiliencia.pdf). Además, en paralelo a la elaboración del PRTR y conscientes de la necesidad de contar con una Administración Pública ágil y eficaz, que sea capaz de garantizar el adecuado destino de los fondos del Instrumento Europeo de Recuperación y su correcta ejecución, en diciembre de 2020, se publicó el Real Decreto-ley 36/2020, de 30 de diciembre, *por el que se aprueban medidas urgentes para la modernización de la Administración Pública y para la ejecución del Plan de Recuperación, Transformación y Resiliencia* [<https://www.boe.es/boe/dias/2020/12/31/pdfs/BOE-A-2020-17340.pdf>].

<sup>58</sup> La modernización de la Administración Pública incluye una hoja de ruta de reformas estructurales entre las que encontramos el IV Plan de Gobierno Abierto 2020-2024 que prevé, entre otros objetivos, la transposición de la Directiva de protección del denunciante al ordenamiento jurídico español.

<sup>59</sup> En nuestro país, aunque existen algunas legislaciones autonómicas que han regulado marcos de integridad y canales de denuncia, su implementación generalizada aún no se ha producido. En estos momentos, a nivel autonómico, se encuentran en funcionamiento la Oficina Antifraude de Catalunya, creada por la Ley 14/2008, de 5 de noviembre [<https://www.boe.es/buscar/pdf/2008/BOE-A-2008-19527-consolidado.pdf>]; la Agencia de Prevención y Lucha contra el Fraude y la Corrupción de la Comunitat Valenciana, creada por la Ley 1/2016, de 28 de noviembre [<https://www.boe.es/buscar/pdf/2016/BOE-A-2016-12048-consolidado.pdf>]; la Oficina de Prevención y Lucha contra la Corrupción en las Illes Balears, regulada en la Ley 16/2016, de 9 de diciembre

Hemos de recordar, no obstante, que la aplicación de sistemas de gestión de irregularidades y la incorporación de mecanismos de prevención y detección del fraude y la corrupción no es una novedad en el marco de la financiación europea. Incluso, desde el año 2017, los Estados Miembros cuentan con orientaciones sobre la forma de comunicar hechos que puedan ser constitutivos de fraude o irregularidad en relación con proyectos u operaciones financiados total o parcialmente con cargo a fondos procedentes de la Unión Europea, pero, hasta ahora, tan solo con carácter de recomendación<sup>60</sup>.

La verdadera dificultad se encuentra ahora, para las entidades perceptoras o ejecutoras de los nuevos fondos, en conciliar las exigencias de la política antifraude del PRTR con los altos estándares de la Directiva Europea de reciente transposición a nuestro ordenamiento ya que no parece que se hayan diseñado de forma conjunta y coordinada por los Ministerios responsables sino, más bien, parece que se podrían llegar a superponer canales, autoridades y procedimientos<sup>61</sup>.

Con el nuevo Reglamento por el que se establece el MRR, y las disposiciones que trasladan al sistema normativo español sus condiciones en esta materia concreta<sup>62</sup>, se identifica como prioritaria

---

[<https://www.boe.es/buscar/pdf/2017/BOE-A-2017-267-consolidado.pdf>]; la Oficina de Buenas Prácticas y Anticorrupción de la Comunidad Foral de Navarra, creada por Ley Foral 7/2018, de 17 de mayo [<https://www.boe.es/buscar/pdf/2018/BOE-A-2018-7644-consolidado.pdf>]; y la Oficina Andaluza contra el Fraude y la Corrupción, creada por la Ley 2/2021, de 18 de junio [<https://www.boe.es/buscar/pdf/2021/BOE-A-2021-11380-consolidado.pdf>]. A nivel municipal, destacan la Oficina para la Transparencia y las Buenas Prácticas del Ayuntamiento de Barcelona y la Agencia de Transparencia del Área Metropolitana de Barcelona, creadas ambas en 2015, y la Oficina Municipal contra el Fraude y la Corrupción del Ayuntamiento de Madrid, creada por Acuerdo del Pleno del Ayuntamiento de 23 de diciembre de 2016 en funcionamiento desde enero de 2018. Encontramos un análisis pormenorizado del caso de Castilla y León en HEREDERO ORTIZ DE LA TABLA (2022).

<sup>60</sup> La Comunicación 1/2017, de 6 de abril, *sobre la forma en la que pueden proceder las personas que tengan conocimiento de hechos que puedan ser constitutivos de fraude o irregularidad en relación con proyectos u operaciones financiados total o parcialmente con cargo a fondos procedentes de la Unión Europea*, tiene por objeto el establecimiento de orientaciones sobre la forma en la que pueden proceder aquellas personas que tengan conocimiento de hechos que puedan ser constitutivos de fraude o irregularidad en relación con proyectos u operaciones financiados total o parcialmente con cargo a fondos procedentes de la Unión Europea, y que deseen ponerlo en conocimiento de la Administración a efectos de que las autoridades competentes puedan realizar las actuaciones necesarias para la investigación o verificación de dichos hechos, y, en su caso, para la tramitación de los procedimientos legalmente establecidos a efectos de exigir las responsabilidades que en cada caso procedan. Se puede consultar en <https://www.igae.pap.hacienda.gob.es/sitios/igae/es-es/snca/Documents/Comunicacion.SNCA06-04-2017Canaldenuncias.pdf>.

<sup>61</sup> El apartado 4.6.8 del PRTR “coordinación en materia de lucha contra el fraude” otorga al Servicio Nacional de Coordinación Antifraude un papel esencial en el modelo, como “órgano estatal encargado de coordinar las acciones encaminadas a proteger los intereses financieros de la Unión Europea contra el fraude en colaboración con la Oficina Europea de Lucha contra el Fraude (OLAF), siendo específicamente designado por el Real Decreto-ley 36/2020, mediante los siguientes elementos: Seguimiento de las sospechas de fraude comunicadas por los órganos gestores, la Autoridad responsable o la Autoridad de control; Fortalecimiento de los medios asignados para la investigación de denuncias a través del canal externo existente; Actuaciones de formación en la materia a los órganos gestores; Coordinación con la Oficina Europea de Lucha contra el Fraude (OLAF) y con la Fiscalía Europea en materia de fraude” y le encomienda la gestión de un canal específico de denuncias que podría entrar en colisión, o al menos objeto de solapamiento, con el canal externo atribuido a la Autoridad Independiente de Protección del Informante. O, a título de ejemplo, el formulario de denuncias por riesgo de fraude incluido en el Plan de Medidas Antifraude para la gestión de los Fondos *Next Generation* UE del Ministerio de Universidades exige la identificación del denunciante y su presentación a través de un correo electrónico al buzón de denuncias del Ministerio, con indicación de su tratamiento confidencial y seguro y de la protección frente a represalias garantizada pero sin observar las exigencias y condiciones previstas en la Directiva Europea y en la ley española respecto a la posibilidad del anonimato.

<sup>62</sup> Los tres instrumentos normativos que permiten la implementación de los compromisos asumidos con la Comisión Europea en el PRTR son: El Real Decreto-ley 36/2020, de 30 de diciembre, por el que se aprueban medidas urgentes para la modernización de la Administración Pública y para la ejecución del Plan de Recuperación, Transformación y Resiliencia; la Resolución de 29 de abril de 2021, de la Subsecretaría, por la que se publica el Acuerdo del Consejo de Ministros de 27 de abril de 2021, por el que aprueba el Plan de Recuperación, Transformación y Resiliencia; y la ORDEN HFP/1030/2021, de 29 de septiembre, por la que se configura el sistema de gestión del Plan de Recuperación, Transformación y Resiliencia y las orientaciones para el refuerzo de los mecanismos para la prevención, detección y corrección del fraude, la corrupción y los conflictos de intereses, referidos en el artículo 6.



la necesidad de establecer canales de denuncias eficaces para la prevención, detección y corrección de los riesgos de fraude.

El MRR reconoce la necesidad de “mejorar la eficacia de la Administración Pública y de los sistemas nacionales, incluida la reducción a un mínimo de la carga administrativa, y la eficacia de los sistemas judiciales, así como la prevención del fraude y la supervisión de la lucha contra el blanqueo de capitales y recopilando categorías armonizadas de datos e información que permita prevenir, detectar y corregir irregularidades graves, tales como el fraude, la corrupción y los conflictos de intereses en lo que respecta a las medidas financiadas por el Mecanismo”.

La necesidad de garantizar el adecuado destino de los fondos y para ello, la mejora en la prevención y lucha contra el fraude por parte de los Estados Miembros es un imperativo. Es por ello que se exige que los Planes Nacionales incluyan una explicación detallada de las medidas propuestas o adoptadas en esta materia<sup>63</sup>.

Así, el PRTR español dedica uno de sus cinco apartados a la “Implementación y Complementariedad del Plan” y, dentro de este, 17 folios de los 348 que conforman el Plan y sus Anexos al “control y auditoría” donde se define un nuevo sistema de control que, además de garantizar el cumplimiento de hitos y objetivos, persigue la finalidad expresa de prevenir, detectar y corregir las irregularidades relativas al fraude, corrupción, conflictos de intereses o doble financiación<sup>64</sup>.

Estas exigencias derivan en el reconocimiento expreso, como principio de buena gestión de las Administraciones Públicas involucradas en la ejecución del PRTR (o principios de consideración obligatoria en la terminología europea) la prevención eficaz de los conflictos de interés, el fraude y las irregularidades<sup>65</sup> y en la atribución a la Intervención General del Estado (IGAE) el papel de Autoridad de Control del MRR y al Servicio Nacional de Coordinación Antifraude (SNCA) las labores de prevención, detección e investigación del fraude que sean precisas, manteniendo a estos efectos las relaciones necesarias con los órganos de gestión y control a los que les corresponderá evaluar las acciones desarrolladas para identificar, en su caso, las desviaciones ocurridas y adoptar las correcciones necesarias así como la gestión del canal de denuncias específico creado para tal fin.

---

<sup>63</sup> Su considerando 15, 39 y 40 así lo establecen identificando claramente el nivel de responsabilidades exigidas al entender que “la Comisión debe velar por la protección efectiva de los intereses financieros de la Unión. Si bien es principalmente responsabilidad del propio Estado miembro garantizar que el Mecanismo se ejecute de conformidad con el Derecho de la Unión y nacional pertinente”. En particular, su artículo 22 recoge la obligación ya que “al ejecutar el Mecanismo, los Estados miembros, en su condición de beneficiarios o prestatarios de fondos en el marco del Mecanismo, adoptarán todas las medidas adecuadas para proteger los intereses financieros de la Unión y para velar por que la utilización de los fondos en relación con las medidas financiadas por el Mecanismo se ajuste al Derecho aplicable de la Unión y nacional, en particular en lo que se refiere a la prevención, detección y corrección del fraude, la corrupción y los conflictos de intereses”.

<sup>64</sup> El Apartado IV referido a la Implementación y complementariedad del PRTR, en su subapartado 4.6, se dedica a definir los mecanismos de control y auditoría que deben observarse: “El sistema de control global e integrado descansa en la estructura organizativa, los mecanismos y herramientas del control ordinario de los gastos públicos, vinculándose a la estructura presupuestaria y al Sistema de Información Contable, tanto en términos de ejecución financiera como de consecución de hitos y objetivos, pero ajustando estos elementos a los especiales requerimientos del Plan, en especial la prevención, detección y corrección del fraude y la corrupción, el conflicto de intereses y la doble financiación, con tres niveles o líneas de defensa. En primer lugar, el control por los propios gestores y los sistemas de apoyo, con un sistema informático integrado de gestión del Plan, que permitirá el almacenamiento y el seguimiento de toda la información relacionada, así como la articulación con los sistemas de control de la Comisión (ARACHNE), facilitando también el acceso a esta información de los órganos de control de la Comisión, la Oficina Europea de Lucha contra el Fraude (OLAF), fiscalía o Tribunal de Cuentas Europeo. Un segundo nivel encomendado a órganos independientes de la propia gestión (servicio jurídico, IGAE y otros órganos de control interno). Y un tercer nivel, de control ex-post mediante auditorías, siendo la Intervención General de la Administración del Estado (IGAE) la Autoridad de Control del Mecanismo de Recuperación y Resiliencia”.

<sup>65</sup> El artículo 3. 2. del Real Decreto-Ley 36/2020 de 30 de diciembre recoge los principios de buena gestión que deben observar las Administraciones Públicas para la ejecución del PRTR y el artículo 2.2.d) de la Orden HFP/1030/2021, de 29 de septiembre establece los principios de gestión específicos del PRTR entre los que se incluye el refuerzo de mecanismos para la prevención, detección y corrección del fraude, la corrupción y los conflictos de interés.

Es importante recordar que el PRTR es una manifestación de compromisos e intenciones generales presentada a las autoridades europeas que, en muchos casos, para hacerse efectiva deberá contar con un desarrollo específico posterior tanto en su vertiente normativa como operativa y que, en muchos casos, a pesar de la relevancia cuantitativa del mecanismo, esto todavía no se ha producido<sup>66</sup>.

A la vista de las dificultades presentadas y de la complejidad y novedad del mecanismo, una de las primeras decisiones que se adoptaron fue la adaptación de los procedimientos de gestión que utilizaban las Administraciones Públicas con el objetivo de poder cumplir con los requerimientos del MRR y de sus modelos de control para facilitar la tramitación eficaz de las solicitudes de desembolso de fondos a los Servicios de la Comisión Europea, desarrollando un sistema de gestión propio del PRTR<sup>67</sup>.

Este sistema de gestión determina que toda entidad decisora o ejecutora de las medidas del PRTR debe disponer de un Plan de Medidas Antifraude, que le permita garantizar y declarar que los fondos correspondientes se han utilizado de conformidad con las normas aplicables, en particular, en lo que se refiere a la prevención, detección y corrección del fraude, la corrupción y los conflictos de intereses. Esta exigencia se justifica al no haber sido contemplados estos principios en la dinámica de la gestión tradicional con el alcance requerido.

En el marco de estas responsabilidades<sup>68</sup>, y sin perjuicio de que cada entidad responsable de la gestión de los fondos puede elegir medidas de prevención y detección específicas atendiendo a sus especiales características y teniendo en cuenta la necesaria garantía de una conveniente protección de los intereses de la Unión, la normativa española establece como actuaciones obligatorias para los órganos gestores: la evaluación de riesgo de fraude, la cumplimentación de la Declaración de Ausencia de Conflicto de Intereses (DACI) y la disponibilidad de un procedimiento para abordar conflictos de intereses.

Para la evaluación de riesgo de fraude, en lo que aquí nos interesa al encontrarse íntimamente relacionada con la implementación de canales de denuncias que permitan comunicar la información relevante, se proporciona una matriz de riesgos o esquema de autoevaluación de diversos aspectos críticos para asegurar un cumplimiento adecuado y homogéneo de los requerimientos establecidos por la normativa comunitaria, sobre la base de una serie de preguntas relativamente sencillas, pero con gran trascendencia.

El análisis se estructura en dos bloques: uno calificado como aspectos esenciales, con la finalidad de identificar la cobertura o no de los mismos en la estructura orgánica y en los procedimientos y, un segundo bloque, sobre cada uno de los aspectos que se consideran críticos con el objetivo de graduar el nivel de adecuación de la estructura orgánica y de los procedimientos disponibles a las

---

<sup>66</sup> En concreto, el Sistema de Información COFFEE (Plataforma Común de Fondos Europeos, módulo del Mecanismo de Recuperación y Resiliencia) que es el sistema de información de gestión del PRTR, clave para ejercer un adecuado control del fraude según el propio PRTR, no se encuentra totalmente desplegado en la actualidad (febrero de 2023) a pesar de que las entidades ejecutoras a las que se les exige la justificación de hitos y objetivos hayan comenzado a recibir fondos en 2021. Toda la información se puede consultar en <https://www.fondoseuropeos.hacienda.gob.es/sitios/dgpmrr/es-es/Paginas/CoFFEE.aspx>. Las últimas críticas recibidas por parte de la Conferencia de Rectores de las Universidades Españolas (CRUE) alertan, incluso, de la posibilidad de la pérdida de los fondos MRR concedidos por defectos en su justificación. Véase la noticia en *CRUE alerta de la paralización de la investigación financiada con fondos europeos por la indefinición de los procedimientos* [<https://www.crue.org/2023/06/paralizacion-investigacion-fondos-europeos-por-indefinicion-de-procedimientos/>].

<sup>67</sup> La Exposición de Motivos y el artículo 6 de la ORDEN HFP/1030/2021, de 29 de septiembre, *por la que se configura el sistema de gestión del Plan de Recuperación, Transformación y Resiliencia* [<https://www.boe.es/buscar/pdf/2021/BOE-A-2021-15860-consolidado.pdf>], se refiere a este aspecto en particular.

<sup>68</sup> Es que el Reglamento del MRR expresa la necesidad de establecer mecanismos reales de control al disponer: “Los responsables y gestores de las medidas deberán asumir el desarrollo de las tareas necesarias para la consecución de los objetivos, en el marco de recursos y costes estimados, el análisis sistemático de la gestión, sustentado en indicadores operativos que faciliten la identificación de los riesgos y la toma de decisiones para el adecuado desarrollo de la actividad”.

necesidades, induciendo una reflexión sobre los aspectos que, a priori, serían determinantes para abordar con solvencia los requerimientos del PRTR.

El procedimiento de autoevaluación termina con la cuantificación del riesgo a partir de las respuestas a los cuestionarios. En caso de que el riesgo sea medio o alto, la entidad afectada debe adoptar medidas orientadas a mejorar los requerimientos que subyacen en las distintas cuestiones que se plantean en los test hasta conseguir una calificación de riesgo bajo en todos los ítems analizados.

La norma establece, además, un procedimiento específico para el caso de detectar un posible fraude o tener una sospecha fundada de ello incluyendo una evaluación de su incidencia y su calificación como puntual o sistémico lo que, además, puede dar lugar a consecuencias correctivas importantes o incluso a la descertificación de los fondos. Es por ello que, dentro de los requerimientos mínimos de todo Plan de Medidas Antifraude, figura la necesidad de contar con mecanismos claros de comunicación de las sospechas de fraude. La implementación de un adecuado canal de denuncias, que proporcione información sistemática y se encargue de su gestión documental, puede ser de gran ayuda<sup>69</sup>.

Las Orientaciones para el Refuerzo de los mecanismos para la prevención, detección y corrección del fraude, la corrupción y los conflictos de intereses elaboradas por la Secretaría General de Fondos Europeos, dependiente del Ministerio de Hacienda y Función Pública, de 24 de enero de 2022, ofrecen una guía práctica para la aprobación de los Planes de Medidas Antifraude por parte de las entidades decisoras y ejecutoras de los Fondos del MRR, ayudándonos en este proceso de diseñar “mecanismos claros de comunicación de sospechas de fraude”.

En la fase preventiva, se reconoce directamente la importancia de los canales de denuncia cuando se establece la necesidad de fomentar valores como la integridad, objetividad, rendición de cuentas y honradez y de recogerlos en un código de conducta ante el fraude que pueda incluir aspectos como el conflicto de interés, los obsequios, la confidencialidad debida o los cauces de denuncia (buzón de denuncias y/o enlace al canal de denuncias del SNCA), entre otras. Para ello, las orientaciones recomiendan identificar claramente a los responsables encargados de examinar y comunicar las denuncias de posibles fraudes o irregularidades y practicar una publicidad eficaz del canal de denuncias para garantizar su accesibilidad y uso<sup>70</sup>.

---

<sup>69</sup> Artículo 6.5 de la Orden recoge, entre otros, requerimientos mínimos que deben contener los Planes de Medidas Antifraude: “a) Aprobación por la entidad decisoras o ejecutora, en un plazo inferior a 90 días desde la entrada en vigor de la presente Orden o, en su caso, desde que se tenga conocimiento de la participación en la ejecución del PRTR; b) estructurar las medidas antifraude de manera proporcionada y en torno a los cuatro elementos clave del denominado «ciclo antifraude»: prevención, detección, corrección y persecución; c) prever la realización, por la entidad de que se trate, de una evaluación del riesgo, impacto y probabilidad de riesgo de fraude en los procesos clave de la ejecución del Plan de Recuperación, Transformación y Resiliencia y su revisión periódica, bienal o anual según el riesgo de fraude y, en todo caso, cuando se haya detectado algún caso de fraude o haya cambios significativos en los procedimientos o en el personal; d) definir medidas preventivas adecuadas y proporcionadas, ajustadas a las situaciones concretas, para reducir el riesgo residual de fraude a un nivel aceptable; e) prever la existencia de medidas de detección ajustadas a las señales de alerta y definir el procedimiento para su aplicación efectiva; f) definir las medidas correctivas pertinentes cuando se detecta un caso sospechoso de fraude, con mecanismos claros de comunicación de las sospechas de fraude; g) establecer procesos adecuados para el seguimiento de los casos sospechosos de fraude y la correspondiente recuperación de los Fondos de la UE gastados fraudulentamente”.

<sup>70</sup> Orientación 6.1: Identificación de una unidad/servicio/órgano o unidades/servicios u órganos de la entidad decisoras/ejecutora a la que se le asigna las funciones que se derivan de la elaboración, aplicación y seguimiento del Plan Antifraude y de las medidas en él contenidas, encargada de realizar la evaluación de fraude, examinar las denuncias, evaluar situaciones que puedan ser constitutivas de fraude o corrupción y, en su caso, comunicarlas a las entidades que corresponda, así como proponer medidas correctoras.

Informar al personal de la organización, mediante su publicación en la web de la entidad decisoras o ejecutora, para general conocimiento, de la existencia del canal de denuncias externo habilitado por el SNCA (infofraude), para la comunicación de información sobre fraudes o irregularidades que afecten a fondos europeos, el cual dispone de un apartado específico relativo al Mecanismo de Recuperación y Resiliencia, teniendo en cuenta lo dispuesto en la Comunicación 1/2017, de 6 de abril, sobre la forma en la que pueden proceder las personas que tengan conocimiento de hechos que puedan ser constitutivos de fraude o irregularidad en relación con proyectos u operaciones financiados total o parcialmente con cargo a fondos procedentes de la Unión Europea.

Por su parte, en la detección de los posibles casos de fraude se confirma la importancia de los canales de denuncia cuando reconocen la necesidad de establecer mecanismos adecuados y claros para informar de las posibles sospechas de fraude por quienes los hayan detectado. Para ello, las orientaciones recomiendan el establecimiento de un procedimiento documentado de banderas rojas como instrumento para la identificación y tratamiento de los posibles casos de irregularidad o fraude<sup>71</sup>.

Y, por último, en lo relativo a la corrección y persecución, su relevancia se constata con la referencia a la necesidad de comunicación de los hechos al Servicio Nacional de Coordinación Antifraude para su valoración y eventual comunicación a la Oficina Europea de Lucha contra el Fraude, iniciar una información reservada para depurar responsabilidades o incoar un expediente disciplinario o denunciar los hechos ante la fiscalía y los tribunales competentes. Para ello, las orientaciones recomiendan que los órganos responsables realicen una valoración preliminar sobre la existencia de intencionalidad o no para su remisión a las autoridades competentes sin perjuicio de la posibilidad de utilizar canales de denuncia externos por parte de cualquier ciudadano o empleado público<sup>72</sup>.

No hay duda, por tanto, que los canales de denuncias y la información que con ellos se recopila y gestiona, juegan un papel esencial en las cuatro fases del ciclo antifraude: prevención, detección, corrección y persecución, y que su establecimiento se presenta como un elemento capital de la buena gestión de los fondos europeos, aunque no existe un catálogo de principios, requisitos y condiciones que deba observarse en el diseño e implementación de estos canales de denuncia, por ahora<sup>73</sup>.

### III. MARCO RELACIONAL: LAS BUENAS PRÁCTICAS

Si queremos contribuir a un mejor funcionamiento del sistema jurídico debemos incorporar el mayor uso posible del conocimiento científico disponible, tanto empírico como conceptual, enfocar su análisis de forma interdisciplinar y mostrar interés por las consecuencias sociales de las soluciones dogmáticas.

Por ello, una vez analizado el marco normativo vigente de los canales de denuncias o canales internos y externos de comunicaciones, resulta necesario incorporar a nuestro estudio las aportaciones que nos ofrece la experiencia del sector público, a través del trabajo que realizan las redes de agencias anticorrupción a nivel nacional y europeo y las mejores prácticas del sector privado, recogidas en la estandarización de normas que realiza la Organización Internacional de Normalización (ISO).

---

<sup>71</sup> Orientación 6.2: Elaboración de un catálogo de banderas rojas o indicadores de riesgo para la lucha contra el fraude y la corrupción en el ámbito de actuación de la entidad decisora/entidad ejecutora, con definición del procedimiento a seguir en el caso de que se detecten alguna de esas banderas rojas. Las banderas rojas son señales de alarma, pistas o indicios de posible fraude. La existencia de una bandera roja no implica necesariamente la existencia de fraude, pero sí indica que una determinada área de actividad necesita atención extra para descartar o confirmar un fraude potencial.

<sup>72</sup> Orientación 6.3: No obstante, en el ámbito estricto de sus funciones, los órganos administrativos deben realizar, sobre la base de la documentación de que dispongan, una valoración preliminar sobre la posible existencia de tal intencionalidad o, en su caso, sobre la ausencia de la misma, de cara a decidir si una determinada conducta debe ser remitida a dichos órganos jurisdiccionales o al Ministerio Fiscal para que sea investigada y, en su caso, sancionada penalmente. En relación con la comunicación del SNCA, se ha de recordar que tanto los ciudadanos como los empleados públicos, en caso de indicios de fraude que afecten a fondos europeos, por debilidades o falta de operatividad en los sistemas de comunicación interna, podrán comunicar los indicios de fraude o los hechos presuntamente fraudulentos al SNCA a través del Canal de denuncias externo Infofraude para su valoración y eventual comunicación a la Oficina Europea de Lucha contra el Fraude.

<sup>73</sup> Resulta interesante citar en este punto la visión sistémica de FERNÁNDEZ AJENJO (2022) del ciclo de lucha antifraude que, partiendo de una nueva denominación de las cuatro fases clásicas, como fase de prevención, inteligencia, investigación y represión, establece una red interrelacionada de instrumentos organizativos y operativos como una maquinaria engrazada de forma rotaria.



## 1. La experiencia de las agencias encargadas de la lucha contra el fraude en el contexto de la cooperación nacional y europea

En España, contamos con varias oficinas y agencias antifraude a nivel nacional, autonómico y municipal y con órganos, con mayor o menor nivel de independencia y autonomía, encargados de la lucha contra el fraude y la corrupción y de la gestión de los canales de denuncia.

En junio de 2018, se constituyó una red nacional, como marco estable de colaboración entre todas las agencias creadas en España hasta ese momento<sup>74</sup>, con la que poder diseñar estrategias compartidas en la lucha contra el fenómeno de la corrupción, unificar criterios de actuación con pleno respecto a la independencia de cada institución, compartir metodologías de formación y prevención y experiencias concretas con las que reforzar la eficacia de sus actuaciones así como, en última instancia presionar con propuestas e iniciativas para conseguir la puesta en marcha de un plan nacional contra la corrupción.

El último encuentro de la Red, en abril de 2023 en Sevilla, los miembros actuales acordaron elevar una propuesta de enmiendas al proyecto de Ley reguladora de la protección de personas que informen sobre infracciones normativas y de lucha contra la corrupción que, en gran parte de su contenido, fue tomado en consideración por el legislador<sup>75</sup>.

En el ámbito europeo, de manera especializada, también contamos con foros independientes para la cooperación institucional, el intercambio de experiencias y la recopilación de buenas prácticas en materia de lucha contra la corrupción.

En 2008, el Consejo de la Unión Europea crea la Red Europea de Puntos de Contacto contra la Corrupción (EANC por sus siglas en inglés) con el objetivo de prevenir y combatir la corrupción. Esta red engloba a todas las autoridades y agencias encargadas de la lucha contra el fraude de los Estados Miembros, incluida la Oficina Europea de Lucha contra el Fraude (OLAF), y en la misma participan la Comisión Europea, Europol y Eurojust como asociados y la Fiscalía Europea Anticorrupción como observador.

La EANC funciona de forma coordinada con otra red preexistente en el ámbito europeo, los Socios Europeos Contra la Corrupción (EPAC según sus siglas en inglés) creada en 2004 por autoridades anticorrupción y órganos de vigilancia policial de países miembros del Consejo de Europa<sup>76</sup>.

---

<sup>74</sup> Las agencias y entidades anticorrupción españolas existentes en aquel momento acordaron, en un encuentro celebrado en la sede de la Oficina Antifraude de Cataluña el 29 de junio de 2018, la creación de esta red. Este primer encuentro, que se ha ido repitiendo anualmente y que ha incorporado nuevos socios, reunió a los máximos responsables de la Oficina Antifraude de Cataluña, Miguel Ángel Gimeno, al director de la Oficina Antifraude de Cataluña, Miguel Ángel Gimeno; el Director de la Agencia de Prevención y Lucha contra el Fraude y la Corrupción de la Comunidad Valenciana, Joan Llinares, al director de la Oficina de Prevención y Lucha contra la Corrupción en las Islas Baleares, Jaime Far, al Conselleiro del Consejo de Cuentas de Galicia, Constantino Carreiras, al director de la Oficina Municipal contra el Fraude y la Corrupción del Ayuntamiento de Madrid, Carlos Granados, y a las responsables de la Oficina para la Transparencia y las Buenas Prácticas del Ayuntamiento de Barcelona: la directora de servicios de Control de Gestión, María del Mar Giménez-Salinas, y la directora de servicios de Análisis de la misma institución, Rosa María Sánchez.

<sup>75</sup> Toda la Información sobre el resultado del encuentro, así como la relación actualizada de representantes que participan activamente en la red, se puede consultar en <https://www.antifraude.es/la-red-estatal-de-oficinas-y-agencias-antifraude-se-reune-en-sevilla-para-analizar-la-aplicacion-de-la-nueva-ley-2-2023-de-proteccion-de-personas-denunciantes-de-corrupcion/>.

<sup>76</sup> La EPAC o la *European Partners against Corruption*, en estos momentos, es la red más grande de Europa en materia anticorrupción, reúne a 90 autoridades anticorrupción y órganos de supervisión policial del Consejo de Europa y de Estados Miembros de la Unión Europea y es una organización especial porque aglutina a diferentes tipos de servicios, agencias, organizaciones, las cuales representan los sistemas de lucha contra la corrupción de cada país.

La membresía en los Socios Europeos contra la Corrupción (EPAC) está abierta a las organizaciones de competencia nacional y/o amplia jurisdicción dentro de los Países Miembros del Consejo de Europa que se ocupan de la supervisión independiente de la policía y de la prevención y la lucha contra la corrupción. También pueden ser miembros organizaciones y redes europeas con objetivos similares. Las autoridades anticorrupción y los organismos de supervisión policial de otros países europeos, así como las organizaciones y redes europeas con objetivos similares, pueden calificarse como observadores. La red europea de puntos de contacto contra la corrupción (EACN) reúne a cerca de 60 autoridades anticorrupción de los Estados miembros de la Unión Europea y a la OLAF. Toda la información se puede consultar en <https://www.epac-eacn.org/about>.

Así, con el objetivo general de fortalecer la cooperación, la EPAC/EACN proporciona una plataforma para que los profesionales intercambien experiencias, información e inquietudes en la esfera de la anticorrupción y la vigilancia policial, se ayuden mutuamente y cooperen más allá de las fronteras nacionales, tanto a nivel de conocimientos teóricos como de experiencias prácticas y sobre la base de estándares éticos que aseguren el respeto por el estado de derecho y los derechos humanos.

Uno de los socios más activos en ambas redes es la Agencia de Prevención y Lucha contra el Fraude y la Corrupción de la Comunitat Valenciana (AVAF). La AVAF, es la segunda agencia más antigua en España y participa activamente desde su creación en las iniciativas nacionales y europeas. Además, destaca por su excelente política de comunicación y difusión lo que permite que tanto su labor como su experiencia práctica sean totalmente accesibles a la ciudadanía y a los poderes públicos<sup>77</sup>.

Es por ello que, a modo representativo y en aras de facilitar el análisis de la experiencia de las diferentes oficinas y agencias, vamos a destacar su trabajo en materia de canales de denuncias, no solo como inspiración para la formulación de los principios generales que deben observarse en el diseño e implantación de canales de denuncia en el ámbito público sino como ejemplo de buenas prácticas que en el contexto nacional y europeo han conseguido resolver los principales dilemas jurídicos y procedimentales que se plantean en esta materia.

En 2018 se crea el buzón de denuncias de la AVAF<sup>78</sup> y se pone a disposición de la ciudadanía en general, y de las personas al servicio de las administraciones públicas en particular, con el objetivo de facilitar la comunicación de posibles casos de uso o destino irregular de fondos públicos y de conductas contrarias a la integridad, cuando se refieran o afecten a entidades e instituciones

---

<sup>77</sup> La Agencia de Prevención y Lucha contra el Fraude y la Corrupción de la Comunitat Valenciana se creó mediante Ley 11/2016, de 28 de noviembre, de la Generalitat Valenciana, modificada por la Ley 27/2018, de 27 de diciembre, de medidas fiscales, de gestión administrativa y financiera y de organización de la Generalitat [<https://www.boe.es/buscar/pdf/2016/BOE-A-2016-12048-consolidado.pdf>], se encuentra adscrita a las Cortes y se configura como entidad con personalidad jurídica propia y plena capacidad de obrar. Su personal es exclusivamente funcionario de carrera procedente de las diferentes administraciones públicas por mandato legal y, en el caso de tener atribuidas competencias inspectoras, gozan de la condición de autoridad pública para el ejercicio de sus funciones.

La Agencia es un instrumento de prevención, investigación y combate del fraude y la corrupción, con capacidad para proteger a las personas denunciantes que comenzó su actividad en julio de 2017 con una plantilla inicial de 32 funcionarios de carrera.

El ámbito de actuación de la Agencia Valenciana Antifraude, que es exclusivamente público, alcanza a: (i) la administración de la Generalitat, el Consell, su Presidencia y las Consellerias; (ii) el sector público instrumental de la Generalitat: organismos autónomos de la Generalitat, entidades públicas empresariales de la Generalitat y otras entidades de derecho público entre las que se encuentran sociedades mercantiles, fundaciones de sector público y consorcios adscritos a la Generalitat; (iii) Les Corts Valencianes, el Síndic de Greuges, la Sindicatura de Comptes, el Consell Valencià de Cultura, la Acadèmia Valenciana de la Llengua, el Comité Econòmic i Social, el Consell Jurídic Consultiu y cualquier otra institución estatutaria análoga que se pueda crear en el futuro, con relación a su actividad administrativa y presupuestaria; (iv) las entidades integrantes de la administración local de la Comunitat Valenciana y las entidades del sector público vinculadas o dependientes; (v) las universidades públicas valencianas y las entidades del sector público vinculadas o dependientes; (vi) las corporaciones de derecho público, en cuanto a las actividades sujetas a derecho administrativo; (vii) las asociaciones constituidas por las administraciones públicas, los organismos y las entidades públicas; (viii) las actividades de personas físicas o jurídicas que sean concesionarias de servicios o receptoras de ayudas o subvenciones públicas, a los efectos de comprobar el destino y el uso de las ayudas o las subvenciones; (ix) las actividades de contratistas y subcontratistas que ejecuten obras de las administraciones públicas y de las entidades del sector público instrumental de la Generalitat o que tengan atribuida la gestión de servicios públicos con relación su gestión contable, económica y financiera y con las otras obligaciones que se derivan del contrato o de la ley; (x) los partidos políticos, las organizaciones sindicales y las organizaciones empresariales; y (xi) cualquier entidad, independientemente de la tipología o la forma jurídica, que esté financiada mayoritariamente por las administraciones públicas o esté sujeta al dominio efectivo de éstas.

Toda la información sobre la AVAF se puede consultar en <https://www.antifraucv.es/que-es-la-agencia-valenciana-antifraude/>.

<sup>78</sup> Se puede consultar en la Resolución de 25 de abril de 2018, del director de la Agencia de Prevención y Lucha contra el Fraude y la Corrupción de la Comunitat Valenciana, por la que se crea el Buzón de Denuncias de la Agencia y se regula su funcionamiento [2018/4529] [[https://www.antifraucv.es/wp-content/uploads/2021/03/2018\\_4529.pdf](https://www.antifraucv.es/wp-content/uploads/2021/03/2018_4529.pdf)].

del sector público de la Comunidad Valenciana. El buzón también se configura como la oficina virtual del empleado público, para permitir a este personal, de forma confidencial, comunicar irregularidades administrativas de las que puedan tener conocimiento en el ejercicio de sus funciones.

Además, con el objetivo de facilitar la implementación y puesta en marcha del canal interno de información exigido por la Ley 2/2023, la AVAF ofrece a las entidades incluidas en su ámbito de actuación la posibilidad de suscribir protocolos de colaboración para asesoramiento, colaboración en su implementación y utilización gratuita del software libre de gestión que utiliza la Agencia para sus buzones de denuncias al ser tecnologías que cumplen todos los requisitos requeridos por la nueva normativa<sup>79</sup>.

El buzón de denuncias de la AVAF funciona como canal externo de denuncias relacionadas con el sector público valenciano y funcionará como canal de externo de comunicaciones previsto en la Ley de protección del informante, aunque, recordemos, su actividad no se extiende a las conductas detectadas en el sector privado.

Aun cuando las denuncias son voluntarias, la ley de creación de la Agencia establece un deber para los empleados públicos afectados de poner en conocimiento los hechos, de forma inmediata, sin perjuicio de las obligaciones de notificación propias de la legislación procesal penal y sin que esto suponga que se adquiere, sin más, la condición de interesado. De esta manera se está tratando de reforzar el establecimiento de una cultura ética y de integridad en el seno de las administraciones públicas a la vez que se deja constancia de la independencia de esta vía respecto de las clásicas establecidas en la legislación penal o administrativa preexistentes.

Es importante recordar que la Agencia no tiene competencias en las funciones y materias que corresponden a la autoridad judicial, el Ministerio Fiscal y la Policía Judicial, ni puede investigar los mismos hechos que han sido objeto de sus investigaciones o que impliquen al sector privado. Junto al escrito de denuncia, se debe adjuntar una declaración expresa y responsable del denunciante de que sobre los mismos hechos no se ha presentado denuncia ante las autoridades judiciales, el Ministerio Fiscal o la Policía Judicial, ni se tiene constancia de la existencia de investigaciones judiciales o policiales sobre los mismos para evitar los supuestos de la referida prejudicialidad penal.

Las denuncias podrán presentarse con identificación de los datos del denunciante o de forma anónima y, en ambos casos, se procederá al análisis del contenido y comprobación de la verosimilitud de la comunicación practicando para ello las actuaciones necesarias.

Por cada comunicación realizada, el buzón asigna un código alfanumérico a través del cual la persona informante puede acceder al sistema e interactuar con el personal funcionario encargado de la gestión y tramitación del expediente. El uso de un *software* libre o canal seguro de comunicación electrónica adaptado a las necesidades de confidencialidad y anonimato es clave para garantizar el éxito del sistema de gestión<sup>80</sup>.

---

<sup>79</sup> La Guía para la aplicación de la Ley 2/2023, de 20 de febrero, publicada el 28 de marzo por la AVAF, se puede consultar en [https://www.antifraucv.es/wp-content/uploads/2023/03/GULA-AVAF-LEY-2\\_2023\\_\\_.pdf](https://www.antifraucv.es/wp-content/uploads/2023/03/GULA-AVAF-LEY-2_2023__.pdf).

<sup>80</sup> En <https://www.antifraucv.es/comunicaciones-anonimas/> encontramos toda la información necesaria sobre como el anonimato de la comunicación en el entorno digital, también de la dirección IP, que puede identificar a la persona que navega por Internet, se garantiza utilizando una red de anonimización. Según AVAF, “la herramienta más utilizada es la red TOR, un software gratuito y de código abierto que permite mejorar la privacidad y seguridad en Internet. Al conectarse a Internet con TOR, la conexión pasa a través de una serie de túneles cifrados antes de ser encaminada hasta su destino lo que dificulta rastrear la fuente de la información. Así, la identidad de la persona que se conecta al Buzón de Denuncias está protegida. El uso de la red TOR para acceder al buzón es aconsejable o indispensable cuando se tiene el convencimiento o la certeza de riesgo, porque garantiza el anonimato de la persona en el momento de la recepción de la comunicación. No obstante, hay que recordar que quien informa debe preservar, también, el anonimato en el momento de la emisión. En muchas administraciones públicas y redes corporativas en general, los administradores de dichas redes impiden el acceso a la página de descarga de TOR o filtran el tráfico dirigido a ella. Por ello, para utilizar este software puede ser necesario hacerlo desde un ordenador de uso personal. La forma más sencilla de utilizar esta red es descargar e instalar el navegador Tor Browser, que se puede obtener desde la página <https://www.torproject.org/download/download-easy.html.es>”.

Es por ello que, en base a la obligación dispuesta en el artículo 157.3 de la Ley 40/2015, de 1 de octubre, *de Régimen jurídico del sector público*, la AVAF pone a disposición de todas las administraciones interesadas su herramienta de software libre, testada y diseñada a medida para este cometido, para su reutilización evitando así la necesidad de acudir al uso de otras tecnologías privadas comercializadas.

Todas las comunicaciones que se presenten serán tramitadas, salvo aquellas que incurran en falsedad evidente o notoria, y se investigarán aquellas que contengan una descripción suficiente que permita identificar el hecho o la conducta y que estén dentro del ámbito de actuación de la Agencia pudiendo recabarse información adicional a través de este canal seguro de comunicaciones.

No obstante, queda claro que las comunicaciones efectuadas no comportan el inicio de un procedimiento administrativo, ni tampoco producen el efecto de presentación en el registro de entrada de la Agencia, no suponen ejercicio de derecho de petición ni constituyen la presentación de recurso administrativo o reclamación alguna. A la persona que informa o comunica los hechos no le corresponde la condición de persona interesada en un procedimiento administrativo que, como ya hemos visto, es una cuestión criticada por parte de la doctrina.

Con independencia del tratamiento anónimo o no de las denuncias, las actuaciones de la Agencia están sujetas al deber de confidencialidad y secreto y deben asegurar la máxima reserva siendo así que no se podrá facilitar información a las personas que no tengan la condición legal de interesados, ni revelar información sobre las actuaciones realizadas, preservando las garantías del denunciado y el buen fin de los procedimientos judiciales o administrativos a los que pueda dar lugar.

Las comunicaciones deben cumplir una serie de requisitos y estar basadas en la certeza razonable de que la información tiene una especial trascendencia para lograr la integridad y buen gobierno del sector público o bien ayuda a evitar el fraude en el empleo de dinero público<sup>81</sup>.

En el supuesto de denuncias falsas, se acordará el archivo de las actuaciones pudiendo incluso derivarse responsabilidades disciplinarias o penales y dar lugar a una sanción si esta ha generado graves perjuicios para la persona denunciada.

Las denuncias o comunicaciones también pueden ser inadmitidas por falta de competencia, archivadas, remitidas al Ministerio Fiscal o autoridad judicial en el caso de presuntos delitos o, por último, determinar la apertura de actuaciones de investigación, siempre de oficio, por resolución del Director de la Agencia.

El procedimiento de investigación de la Agencia no podrá exceder de seis meses desde que se adoptó la resolución de inicio, pudiendo ampliarse como máximo otros seis meses más, cuando las circunstancias o la complejidad del caso así lo aconsejen y de forma motivada. Para el intercambio de datos e información relevante se firman acuerdos de colaboración con otros órganos e instituciones de supervisión y control y se trabaja de forma coordinada con las instituciones europeas.

La investigación termina con el emisión de un informe motivado de conclusiones que se remite al órgano competente para proceder; con la formulación de recomendaciones o requerimientos concretos para mejorar la detección y prevención del riesgo de conductas irregulares identificadas; con el archivo de las actuaciones; con el inicio de un procedimiento sancionador; con la propuesta al órgano competente de la apertura de procedimiento disciplinario o sancionador; con el traslado al Ministerio Fiscal o autoridad judicial en caso de presuntos delitos; o con la remisión al Tribunal

---

<sup>81</sup> La denuncia debe proporcionar la máxima información de la que disponga la persona denunciante o facilitar las fuentes donde poder obtenerla. En concreto debe contar con una narración clara y cronológica de los hechos y circunstancias que motivan la denuncia, la identificación de la administración o entidad del sector público a la que se refieren o afectan los hechos denunciados; la identificación de la persona o personas presuntamente responsables de los hechos denunciados o que hayan presuntamente participado o colaborado de alguna manera en los mismos; una explicación breve de los pasos ya realizados previamente en relación con los hechos denunciados, como procedimientos o recursos administrativos tramitados, quejas interpuestas ante las administraciones, expedientes disciplinarios, etc.; cualquier otra información que se considere que pueda ser útil para el conocimiento de los hechos denunciados y los posibles responsables. Se facilita un formulario para la presentación de las denuncias, que se puede consultar en <https://www.antifraucv.es/wp-content/uploads/2021/03/MODELO-DENUNCIA-v1.0.pdf>.



de Cuentas en caso de presunta responsabilidad contable o con la presentación a la comisión parlamentaria del correspondiente informe, que puede incluir constancia expresa del incumplimiento injustificado del deber de colaboración, si la relevancia social o la importancia de los hechos lo requieren.

La Dirección de Análisis e Investigación de la Agencia será la responsable de realizar todas estas tareas, en particular la de ejercer la dirección técnica superior del análisis, la investigación y la inspección, además de las de supervisar y velar por el buen funcionamiento del buzón de denuncias. De todas estas actuaciones se realizará un seguimiento, las resoluciones finales de investigación se harán públicas en la web de la Agencia y se dará cuenta a las Cortes en su memoria anual o en el informe extraordinario que se eleve a la comisión parlamentaria correspondiente.

Por último y de forma complementaria a la garantía de un procedimiento seguro de comunicación de irregularidades, debemos referirnos a la protección que se brinda a los informantes a través del estatuto de la persona denunciante por el que las personas que alertan prácticas corruptas reciben de forma inmediata el amparo necesario para evitar represalias de cualquier tipo como aislamiento, persecución o empeoramiento de las condiciones laborales o profesionales o cualquier otra medida que implique cualquier forma de perjuicio o discriminación.

La Dirección de Asuntos Jurídicos de la Agencia presta asesoría legal sobre los hechos relacionados con la denuncia y los procedimientos que se interpongan en su contra con motivo de la misma, velando la protección de las personas denunciadas, informantes y alertadoras, proponiendo la adopción de medidas que garanticen su protección, y en particular para preservar su indemnidad personal y profesional, incluso, una vez terminada la fase de investigación que corresponde a la Agencia.

Sin duda, la confianza que genera el canal de denuncias de irregularidades de la AVAF se sustenta, por un lado, en la autonomía y profesionalidad de su personal y, por otro, en el uso de una tecnología segura que garantiza la confidencialidad y el anonimato de las comunicaciones. Ambas condiciones deberían figurar como condiciones esenciales a la hora de implementar los canales que se introducen como obligatorios en la normativa española.

## **2. La estandarización de las normas como resultado del consenso sobre las mejores prácticas**

La estandarización, normalización o autorregulación no surge del cumplimiento de una obligación legal si no que su esencia radica en la identificación y recopilación de las mejores prácticas del sector privado. Ayuda a resolver grandes debates teóricos sobre aspectos jurídicamente novedosos, armoniza los estándares internacionales y ofrece un modelo uniforme al que las entidades pueden recurrir con gran ahorro de costes de información y de cargas administrativas que, además, les permite diferenciarse fácilmente de las incumplidoras<sup>82</sup>.

Hoy en día, gracias a la intensa capacidad de innovación de los ecosistemas industriales, es cada vez más común la estandarización de procedimientos y el acercamiento entre el Derecho y la técnica<sup>83</sup>. La Unión Europea, consciente de los beneficios que la estandarización genera, acaba de

---

<sup>82</sup> Como acertadamente señalan SÁNCHEZ MACÍAS y RODRÍGUEZ LÓPEZ (2021), “también es necesario que las organizaciones cumplidoras sean reconocidas como tales y puedan diferenciarse de otras que no actúan guiadas por estos valores. En caso contrario, los potenciales problemas de selección adversa pueden esterilizar el intento. Precisamente, ese es el papel llamado a desempeñar por las certificaciones de sistemas de gestión de *compliance*”.

<sup>83</sup> A título de ejemplo, podemos referirnos a la estandarización como algo habitual en el sector químico: combustibles basados en hidrocarburos y biocombustibles así como adhesivos, protectores de la madera, explosivos para uso civil, etc.; construcción e ingeniería civil: estructuras, productos, materiales, equipos pero también resistencia al fuego, geotextiles, etc.; bienes domésticos, deporte y ocio: juguetes, gimnasia, equipamiento deportivo y de las áreas de juego, textiles y fuegos artificiales, etc.; medio ambiente: calidad del agua y del aire, vertederos y eco-etiquetado, etc.; alimentación: análisis de los ingredientes de los alimentos, alimentos para animales, aseguramiento de la calidad, embalaje y logística, etc.; normas generales: acreditación, certificación, ensayos e iluminación, acústica y vibración, etc.; sanidad: productos sanitarios, implantes, productos de diagnóstico y materiales y productos ópticos y dentales, etc.; salud y seguridad: Equipos de protección individual (oídos, ojos y vías respiratorias), etc.; calefacción, refrigeración, ventilación: aparatos a gas, aparatos que utilizan petróleo y combustible sólido, bombas de refrigeración y de calor,

publicar la Estrategia de Normalización de la UE surgida con el objeto reforzar su competitividad a escala mundial, facilitar una economía resiliente, ecológica y digital y consagrar los valores democráticos en las aplicaciones tecnológicas<sup>84</sup>.

La incidencia de las formas de autorregulación normativa en el Derecho, a través de las normas técnicas, se plantea hoy como una oportunidad para los marcos de integridad públicos de la misma manera que ya ha ocurrido en otros ámbitos como, por ejemplo, en el derecho penal económico ya que propicia el cambio cultural a favor del cumplimiento, contribuye a la mejora de la productividad, la competitividad y el crecimiento económico, enriquece el diseño de las políticas públicas y es un ejemplo de éxito de colaboración pública-privada<sup>85</sup>.

La concepción actual de un *compliance* integral, más allá del mero respecto a las leyes y reglamentos, exige un cumplimiento proactivo sometido tanto a controles externos o legales, como internos o basados en compromisos empresariales, éticos o sociales. Este nivel cualificado de cumplimiento se garantizará mediante un adecuado análisis y control de los riesgos y la implementación de una cultura que, insertada en su estrategia, represente el compromiso de la organización<sup>86</sup>.

Una de las mejores maneras de llevar a cabo este *compliance* integral, basado en el control y en la cultura, en el seno de todas las organizaciones es a través de la implantación de los llamados sistemas de gestión<sup>87</sup>. No es casualidad que la norma española reguladora de la protección del informante utilice el concepto de sistema interno de gestión que engloba los diferentes canales de comunicaciones que operan en el seno de la misma organización en lugar de referirse a canales de denuncias internos como elementos aislados del resto del modelo.

Los sistemas de gestión se definen como un conjunto de herramientas básicas para la mejora de la calidad que, perfeccionados a partir de la identificación y depuración de mejores prácticas y sobre la base de las estrategias de mejora continua, con la metodología del ciclo PDCA (Planificar, Hacer, Verificar, Actuar) se vieron consagrados en 1987 con la elaboración por parte de la Organización Internacional de Normalización o Estandarización (ISO) de la primera versión de la norma o estándar ISO 9001 Sistemas de gestión de la calidad<sup>88</sup>.

---

etc.; sociedad de la información: tecnologías de la información y comunicación, el programa eEurope, etc.; materiales: acero, cobre, aluminio, plomo, cinc, y estaño o papel, cuero, textiles y plástico, etc.; ingeniería mecánica: normas de seguridad para maquinaria, especificaciones para equipos a presión, calderas, tuberías, tanques, etc.; medición: contadores de agua, gas y energía térmica o manómetros, etc.; servicios: propósitos contractuales y de formación en transporte, turismo y servicios postales, etc.; transporte y embalaje: interoperabilidad de ferrocarriles convencionales y de alta velocidad, aeronáutica y espacio, transporte de mercancías peligrosas por carretera y por ferrocarril, embalajes y residuos de embalajes, etc.; empresas suministradoras y energía: suministro de gas y agua, ingeniería energética, cogeneración, aguas residuales y sistemas solares térmicos, etc.

<sup>84</sup> La estrategia europea de normalización y su programa de trabajo anual para 2022 se puede consultar en <https://ec.europa.eu/docsroom/documents/48598/attachments/2/translations/en/renditions/native> y <https://ec.europa.eu/docsroom/documents/48601/attachments/3/translations/en/renditions/native>.

<sup>85</sup> Es interesante el enfoque de MONTANER FERNÁNDEZ (2018).

<sup>86</sup> RODRÍGUEZ LÓPEZ y SÁNCHEZ MACÍAS (2021) profundizan en estos conceptos.

<sup>87</sup> Un sistema de gestión puede definirse, según el apartado 3.1 términos y definiciones de la norma UNE-ISO 37002, como un conjunto de elementos de una organización interrelacionados o que interactúan para establecer políticas y objetivos, así como procesos para lograr estos objetivos. Este mismo concepto es utilizado por las normas que adaptan los sistemas existentes a las exigencias del PRTR recientemente publicadas y analizadas en profundidad en el epígrafe anterior.

<sup>88</sup> La Organización Internacional de Normalización (ISO) es una organización no gubernamental internacional con sede en Ginebra, constituida en el año 1947 a partir de la iniciativa de 67 comités técnicos de 25 países del mundo expertos en diferentes disciplinas. Es quizás el organismo de desarrollo de normas más completo y complejo y con mayor reputación. Hoy en día cuenta con 165 miembros, Organismos Nacionales de Normalización habilitados por designación legal en su país.

Su principal función es crear normas o estándares a partir del trabajo de sus comités técnicos compuestos por personal propio y expertos de empresas, organizaciones no gubernamentales, agencias públicas, universidades, centros de investigación y grupos de interés que participan voluntariamente y que buscan obtener el máximo consenso posible. Además, ISO produce otros documentos basados en el consenso y en las buenas prácticas como los documentos de especificaciones técnicas (ISO/TS), informes técnicos (ISO/TR), especificaciones públicamente disponibles

El éxito del planteamiento formulado por ISO radica en que incorporó un enfoque basado en la gestión de los procesos más que en la revisión de los resultados, otorgando de esta manera un papel predominante a la vertiente preventiva o cultural frente a la correctiva o de inspección y en su carácter de modelo de recomendaciones o requisitos para llevar a cabo determinados procesos. Estas directrices no se refieren al mero cumplimiento de obligaciones legales, sino que se elaboran a partir de la consolidación de las mejores prácticas en la materia y, una vez que el sistema es certificado por un organismo externo confiable, permite afirmar que la organización cumple con los más altos estándares, ganándose la confianza de los mercados en los que opera.

En el ámbito específico de los sistemas de gestión de *compliance*, las diferentes normas ISO elaboradas hasta el momento, dado su carácter recopilador de las mejores prácticas en el ámbito de la lucha eficaz contra la corrupción, consensuadas y, además, susceptibles de certificación, no solo generan ventajas reputacionales en el tráfico jurídico a las organizaciones que las implantan, sino que, además, tiene un importante valor social al suponer la instauración de una cultura de integridad.

La primera norma internacional en materia de *compliance*, la ISO 19600 Sistemas de gestión de *compliance*. Directrices, publicado en 2014 y adoptada al catálogo español como UNE-ISO 19600, proporcionaba recomendaciones con el objetivo principal de lograr un cambio en la cultura de cumplimiento de las organizaciones. Varios años después de su publicación, y respondiendo a las necesidades del mercado, en julio de 2021, se vio sustituida por la Norma ISO 37301 Sistemas de gestión de *compliance*. Requisitos, conteniendo una orientación para su uso, que va un paso más allá estableciendo requisitos y configurándose por tanto como una norma de tipo certificable. Esto permite a las organizaciones demostrar ante sus partes interesadas su compromiso de cumplir y su capacidad de reducir al máximo los riesgos a través de una certificación por una tercera parte independiente.

La Norma ISO 37301 complementa otras normas que abordan ámbitos específicos del *compliance*, como la ISO 37001 Sistemas de gestión antisoborno. Requisitos, con orientación para su uso, de abril de 2017, y las certificables UNE 19601 para el *compliance* penal, de mayo de 2017, y la UNE 19602 para el *compliance* tributario, de febrero de 2019, al tiempo que se alinea con la Agenda 2030 de Naciones Unidas, en particular con el ODS 16: Paz, justicia e instituciones sólidas, contribuyendo significativamente a dos de sus metas: reducir la corrupción y el soborno en todas sus formas y crear instituciones eficaces, responsables y transparentes a todos los niveles.

La Norma ISO 37002 Sistemas de gestión de la denuncia de irregularidades. Directrices, aprobada en octubre de 2021 por el comité internacional ISO/TC 309 Gobernanza de las organizaciones, en el que participa España, impulsa los canales de denuncias como herramienta fundamental para el control y la generación de una cultura de *compliance*, ayudando a las

---

(ISO/PAS), acuerdos internacionales de taller (IWA) y guías para difundir su actividad o para ayudar a comprender la actividad que realiza en sectores específicos.

Todos los elementos de las normas ISO responden a una misma estructura (Estructura de Alto Nivel o HLS) para facilitar la implantación de diferentes normas de gestión y necesariamente comprende: objeto y campos de aplicación; referencias normativas; términos y definiciones; contexto de la organización; liderazgo; planificación; apoyo; operación; evaluación del desempeño; y mejora.

Las normas internacionales ISO sobre sistemas de gestión pueden ser de tipo A (especificaciones), con requisitos de carácter certificable, o de tipo B (líneas directrices), con recomendaciones no certificables. En ambos casos se trata de normas de implementación voluntaria por parte de las organizaciones y concebidas como instrumentos de autorregulación.

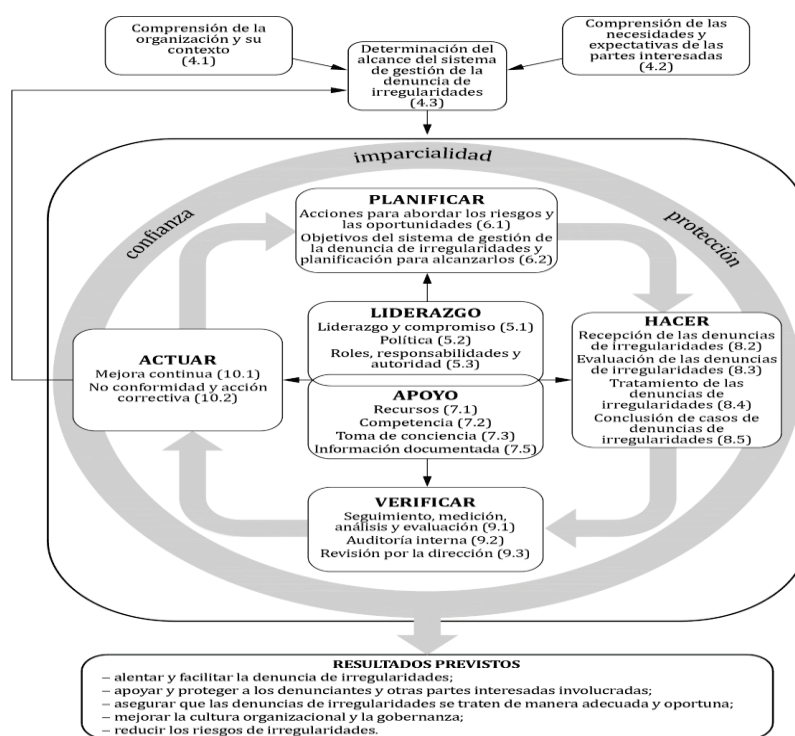
En España, la Asociación Española de Normalización AENOR, desde 1985, y a partir de 2017, Una Norma Española UNE, resultante de la división de AENOR en dos entidades distintas para realizar funciones independientes de normalización y certificación, es el organismo nacional habilitado para participar como miembro de ISO y para funcionar como Organismo de Desarrollo de Normas según la designación realizada por el Ministerio de Economía, Industria y Competitividad como organismo nacional de normalización.

organizaciones a establecer una sólida cultura de integridad y cumplimiento, contribuyendo así a su éxito y sostenibilidad<sup>89</sup>.

Los estudios y la experiencia demuestran que una gran proporción de irregularidades llega al conocimiento de la organización afectada a través de la información que proporcionan las personas de dentro de la organización o cercanas a la misma<sup>90</sup>.

Siguiendo el modelo de normas internacionales ISO y de la práctica norteamericana, especialmente prolífica en la materia, la ISO 37002 rehúye a utilizar conceptos estrictamente jurídicos recurriendo a conceptos de tipo organizativo con el objetivo de dotar de una mayor eficacia a la hora de su aplicación y, con ello, acudir a la fórmula jurídica que mejor encaje en cada caso<sup>91</sup>. Además, es adaptable y su uso variará con el tamaño, naturaleza, complejidad o jurisdicción de las actividades de la organización.

La Norma ISO 37002 ofrece a las organizaciones orientaciones para introducir o mejorar sus sistemas de gestión de denuncias de irregularidades que, basados en los principios de confianza, imparcialidad, protección y retroalimentación, tienen como objetivo alentar y facilitar las denuncias, asegurar que estas se tratan de manera adecuada y oportuna, apoyar y proteger a los denunciantes y reducir el riesgo de que las irregularidades se produzcan a la vez de mejorar la cultura organizacional, la gobernanza y la reputación de las instituciones<sup>92</sup>.



<sup>89</sup> Nuestro país participa activamente a través de los órganos técnicos de normalización CTN/165 SC 1 Gobernanza y canales de denuncia y CTN/165 SC 3 Sistemas de gestión del cumplimiento y sistemas de gestión anticorrupción, cuya secretaría desempeña UNE. Además, parece que la 37002 podrá ver potenciada su eficacia con la futura Norma ISO 37008 Investigaciones internas de las organizaciones. Orientación, que ofrecerá buenas prácticas sobre los principios que han de regir una investigación en todas y cada una de sus fases.

<sup>90</sup> Un análisis más detallado puede verse en nuestro trabajo ARES GONZÁLEZ (2021).

<sup>91</sup> Por ejemplo, acudiendo a la referencia “organización” en lugar de persona jurídica o “función” en lugar de compliance manager se consigue esta aplicación universal de las normas ISO según CASANOVAS YSLA (2018).

<sup>92</sup> Debemos tener en cuenta que con esta misma finalidad encontramos otros instrumentos, como por ejemplo y para el Derecho norteamericano, la Guía del Departamento de Justicia de los Estados Unidos editada para la evaluación de los programas de cumplimiento, de 30 de abril de 2020, establece una serie de criterios a tener en cuenta para validar la eficacia de los programas de cumplimiento normativo y que, en el particular de los canales de denuncia establece la necesidad de que se ocupen de la recepción de irregularidades y otras conductas, a través de procedimientos rigurosos, que respeten la confidencialidad y eviten la posibles represalias y cuenten con personal cualificado, objetivo e imparcial. Se puede consultar en <https://www.justice.gov/criminal-fraud/page/file/937501/download>.



## I. Descripción general de un sistema de gestión de denuncias de irregularidades.

Fuente: <https://www.iso.org/obp/ui/#iso:std:iso:37002:ed-1:v1:es>

El sistema de gestión de denuncia de irregularidades, para que sea eficaz, debe distinguir necesariamente cuatro fases perfectamente planificadas: recepción, evaluación, tratamiento y conclusión de los casos de denuncias de irregularidades.

Para la Norma ISO, la irregularidad puede incluir desde el incumplimiento de la ley, fraude, corrupción, mala administración o abuso de autoridad hasta incumplimiento del código de conducta de la organización. La determinación del tipo de irregularidades que se pueden abordar a través del sistema de gestión de denuncias, así como la relación existente con otros procesos y sistemas que puedan estar previstos para resolver conflictos son dos aspectos importantes para determinar su alcance y efectividad.

La política de denuncia de irregularidades debería formar parte de la política de integridad de la organización y ser aprobada por la alta dirección, desarrollarse con participación del personal y otras partes interesadas y, por supuesto, estar fácilmente disponible, comunicarse periódicamente y revisarse a intervalos planificados.

Los beneficios potenciales que se perciben con la implantación de sistemas de gestión de la denuncia de irregularidades —o canales de denuncias o canales internos de comunicaciones— están relacionados con la identificación temprana de posibles irregularidades y reacción ágil frente a las mismas minimizando o evitando los daños económicos, sociales y reputacionales; la demostración del compromiso sólido al más alto nivel con la cultura de cumplimiento ético y de integridad y la generación, retención y atracción del mejor talento en la organización.

Como ya ocurrió con la Norma ISO 19601, con la que se “ayuda a las organizaciones a desarrollar sistemas de gestión de *compliance* penal con contenidos razonables para prevenir, detectar y gestionar conductas ilícitas generando así la cultura organizativa del cumplimiento de la legalidad que pueda fundamentar, en última instancia, la exoneración de su responsabilidad, aunque siendo conscientes que en el caso de la legislación española, el cumplimiento de esta norma UNE no asegura la exoneración o atenuación automática de la responsabilidad penal de la persona jurídica”, la Norma ISO 37002 puede contribuir a implementar de manera adecuada los canales de denuncia en el ámbito público aunque su contenido se base, por ahora, en meras recomendaciones y no en requisitos<sup>93</sup>.

## IV. PRINCIPIOS GENERALES PARA UN ADECUADO DISEÑO DEL CANAL DE DENUNCIAS PÚBLICO

Teniendo en cuenta las circunstancias descritas en las páginas precedentes y como consecuencia de la indefinición injustificada de algunos aspectos de la reciente normativa publicada y del no siempre efectivo enfoque tradicional, consideramos crucial identificar la manera en que debemos diseñar los canales de denuncias en el ámbito público para que puedan cumplir de manera eficaz su cometido<sup>94</sup>.

---

<sup>93</sup> Para RAGUÉS I VALLÉS (2021), “un nuevo avance en la estandarización de los modelos de prevención de delitos: la ISO 37002 sobre gestión de sistemas de denuncia” 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”.

<sup>94</sup> La denominación “canal de denuncias” se utiliza, en aras de una mejor comprensión del contenido de los principios formulados, como un término paraguas. En cada caso concreto y en función de la normativa o ámbito de aplicación de referencia, deberíamos acudir a las denominaciones “sistema interno de información”, “canal interno o externo de información”, “canal de denuncias interno o externo” o “sistema de gestión de denuncias de irregularidades”.

Con esta finalidad, a continuación presento un catálogo de nueve principios formulado sobre la base de las pautas y procedimientos establecidos en la norma técnica ISO 37002 y de la experiencia reportada por las agencias antifraude que cooperan en redes nacionales y europeas de lucha contra la corrupción, además de, por supuesto, lo contenido en la Directiva de protección de los denunciantes, en la Ley reguladora de protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción o en los requerimientos exigidos por el Mecanismo de Recuperación y Resiliencia para percibir fondos *Next Generation*, que entendemos que deberían observarse para una adecuada implantación del canal de denuncias, especialmente, en las organizaciones públicas. Estos principios son los que estudiamos a continuación.

## 1. Implicación y compromiso al más alto nivel

La implementación del canal de denuncias no solo debe justificarse en el cumplimiento de una obligación legal, sino que debe reconocerse como un mecanismo eficaz para detectar irregularidades y para generar entornos seguros y confiables en los que se fomente una verdadera cultura de cumplimiento. En el diseño e implementación del canal de denuncias resulta esencial la implicación desde la cúpula de la organización (*tone from the top*) definiendo los límites.

El compromiso con la política de integridad y, en concreto, con el sistema de gestión de irregularidades o canal de denuncias, debe demostrarse de forma indubitada, interna y externamente, por el órgano de gobierno y la alta dirección para que produzca el resultado esperado<sup>95</sup>.

## 2. Integración del canal de denuncias en la política de integridad

El órgano de gobierno y la alta dirección, de forma coherente con los propósitos de la entidad y con los riesgos a los que se enfrenta, establecen los objetivos que persigue en particular el canal de denuncias, atribuyen roles y responsabilidades a personas determinadas, con la autonomía e independencia necesarias para llevar a cabo la función de gestión y diseñan los procedimientos oportunos para su implementación y revisión<sup>96</sup>.

El canal de denuncias es un elemento más del sistema formado por el código ético, la política de ausencia de conflicto de intereses o de gobierno abierto, transparencia y rendición de cuentas, entre otras, en el que debe resaltar la consistencia de la política de integridad general y interrelación entre sus distintos componentes<sup>97</sup>.

---

<sup>95</sup> El Apartado 5.1 de la ISO 37002: Liderazgo y compromiso, implica, entre otras funciones de la alta dirección, la de aprobar la política de denuncia de irregularidades y la de comunicar mensajes claros acerca de la existencia, importancia y uso del canal de denuncias. La ley española de protección del informante atribuye en su artículo 5.1 la responsabilidad de la implantación del sistema interno de información al órgano de administración o de gobierno de la entidad y a lo largo de la exposición de motivos de la norma apela al principio de liderazgo.

En el mismo sentido se pronuncian las Recomendaciones del Consejo de la OCDE sobre integridad pública relativa al compromiso —“demostrar compromiso al más alto nivel político y gerencial en el sector público para mejorar la integridad y reducir la corrupción”— y al liderazgo —“invertir en liderar la integridad para que el organismo público demuestre su compromiso”—.

Por su parte, el liderazgo eficaz es uno de los conceptos que deben considerarse en la puesta en marcha de planes de integridad públicos, según la Guía AVAF: El Plan de integridad pública: Hoja de Ruta y Anexos Facilitadores y la implicación de los órganos de gobierno demostrando el compromiso político de la organización es clave para establecer adecuadas dinámicas de implementación según su apartado 2.6.

<sup>96</sup> El Apartado 5.3: roles, responsabilidades y autoridades, el apartado 6.2: objetivos del sistema de gestión de denuncias de irregularidades y planificación para alcanzarlos y el apartado 8.1: planificación y control operacional hacen referencia a la planificación dirigida al más alto nivel, de la ISO 37002 hacen referencia a estos conceptos. En el mismo sentido, pero de manera más esquemática, el artículo 8 de la Ley española de protección del informante se refiere a la figura del responsable del sistema, su designación, funciones y responsabilidades y el artículo 9 describe el procedimiento de gestión de las informaciones.

<sup>97</sup> El Apartado 6.1 de la ISO 37002: Acciones para abordar riesgos y oportunidades, refleja el principio de consistencia de la política de integridad general y el principio de coherencia entre la política de denuncia de irregularidades y el propósito de la organización. Por su parte, la Ley de protección del informante y de lucha contra la corrupción, en su artículo 1, contempla el fortalecimiento de las infraestructuras de integridad en las organizaciones

### 3. Determinación de los riesgos y definición del alcance de la protección

Una vez valorados todos los riesgos potenciales, la organización debe definir con claridad y precisión las conductas susceptibles de ser comunicadas a través del canal de denuncias y los agentes que pueden o deben participar en este proceso de comunicación<sup>98</sup>.

Los sistemas de gestión de la denuncia de irregularidades o canales de denuncias sólo serán eficaces si se extienden a todas las actividades, procesos y miembros de la organización. Resulta esencial determinar, desde el primer momento y con este cometido, todos los riesgos potenciales a los que se enfrenta la entidad, a través de los llamados mapas de riesgos, priorizando sobre ellos las medidas de prevención, detección y reacción o gestión.

Los canales de denuncias deben concebirse como instrumentos tanto para la comunicación de las irregularidades detectadas como para el planteamiento de inquietudes ya que el objetivo de los sistemas de gestión también comprende el cambio cultural y la generación de confianza organizacional<sup>99</sup>.

### 4. Publicidad, difusión y participación

Para garantizar el éxito del canal de denuncias, las personas que trabajan en la organización deben conocer de forma detallada la política de denuncia de irregularidades, sus objetivos, los mecanismos de protección a su alcance y su contribución a la eficacia del sistema o, por el contrario, las implicaciones del incumplimiento. Esta información debe estar documentada y ser fácilmente accesible, además de comunicarse periódicamente en los idiomas, lenguajes y formatos adecuados y transmitirse a todo el personal a través de capacitaciones o formaciones a medida<sup>100</sup>.

---

como una de sus finalidades y en la definición inicial del Sistema interno de Información que hace el artículo 5.2 de la Ley 2/2023, se hace constar la necesidad de contar con una política o estrategia en la materia.

La Guía AVAF: El Plan de integridad pública: Hoja de Ruta y Anexos Facilitadores recomienda, en su apartado 2.4, la fijación del marco conceptual del plan de integridad institucional, como marco de integridad que forma parte de un enfoque estratégico basado en evidencias empíricas y contraste de riesgos y además, en su apartado 2.5, identifica la necesidad de que estos planes, que incluyen los canales de comunicación y los canales de denuncias de irregularidades, deben ser parte integrante de toda la estrategia de integridad de la entidad pública.

<sup>98</sup> El Apartado 4.3 de la ISO 37002: determinación del alcance del sistema de gestión de la denuncia de irregularidades, hace referencia a la necesidad de establecer los límites y la aplicabilidad del sistema de gestión de denuncias de irregularidades por parte de la alta dirección para determinar su alcance. Esto implica considerar el contexto de la organización, las partes interesadas, el ámbito subjetivo y objetivo del canal y los resultados de la evaluación inicial de riesgos.

<sup>99</sup> Este principio se ve claramente comprometido con la concepción del ámbito material de la Ley de protección del informante, en su artículo 2, y con su confusa redacción al incluir no solo las conductas recogidas en la Directiva sino a los ilícitos penales y administrativos graves y muy graves pero, por el contrario, no atender a las irregularidades que pudieran comprometer la integridad de la organización como conductas susceptibles de protección. Es así que el apartado 4 del artículo 7, permite que los canales internos puedan estar habilitados para la recepción de otras comunicaciones o informaciones pero indicando expresamente que en estos casos no se dispone de la protección dispensada por la norma.

La AVAF expresamente reconoce, apartado 2.6.3 de su Guía, la necesidad de que los canales de denuncias integren las comunicaciones de cualquier otro suceso que pueda comprometer cualquier fondo público con independencia de su financiación a pesar de lo que manifiesta la Directiva *whistleblower*. Además, debemos recordar que, en concreto, el buzón de denuncias de la AVAF se configura también como oficina virtual del empleado público, para permitir a este personal, de forma confidencial, comunicar irregularidades administrativas de las que puedan tener conocimiento en el ejercicio de sus funciones.

<sup>100</sup> El apartado 5.2 y el apartado 7.4 y 7.5 de la ISO 37002 hacen referencia a los requisitos de difusión y comunicación de la política de denuncia de irregularidades y el apartado 7.3 identifica como necesaria la toma de conciencia y formación de todas las personas que realizan trabajos bajo el control de la organización, extendiéndose por tanto más allá del personal propio. El título IV de la Ley de protección del informante se dedica a la publicidad de la información y registro de las informaciones y en su artículo 25 se establece, sin más detalle, la obligación de informar de manera clara y accesible sobre el uso del canal interno y los principios esenciales del procedimiento de gestión refiriéndose a que esta información debe estar en la página de inicio de las web existentes pero omitiendo cualquier otra indicación sobre los cauces de publicidad, comunicación o difusión que serían procedentes.

Además, para que esta política sea defendida y practicada por todos los afectados, es conveniente que todas las personas puedan participar en el proceso de formación de la voluntad de la organización y de toma de decisiones, cada uno en los niveles, fases o responsabilidades que le correspondan y que han sido previamente asignadas<sup>101</sup>.

## 5. Suficiencia de recursos

La entidad debe diseñar un canal de denuncias que comprenda cuatro fases diferenciadas: (i) recepción, (ii) evaluación, (iii) tratamiento y (iv) conclusión<sup>102</sup>. Y garantizar que, en todas ellas, las personas responsables cuentan con la autoridad, competencia, integridad e independencia necesarias<sup>103</sup>. Entre otras consideraciones, las personas que ejercitan funciones de inspección tienen que contar con la condición de autoridad para el ejercicio eficaz de su misión.

Es absolutamente necesario que la entidad ponga a disposición recursos materiales suficientes para implementar, operar y mejorar el sistema<sup>104</sup>.

## 6. Tratamiento seguro de la información

La atribución por la alta dirección de las responsabilidades que deben asignarse para el correcto desarrollo de la función de gestión de la denuncia de irregularidades<sup>105</sup> y la determinación de un

---

Según AVAF, apartado tercero de su Guía para la implementación de la Ley 2/2023, las entidades públicas y privadas obligadas por la Ley deberán contar con una política o estrategia que enuncie los principios generales en materia de sistema interno de información y defensa del informante y que sea debidamente publicitada en el seno de la entidad u organismo. La importancia de la información y de la formación práctica a todos los niveles organizativos es destacada en el apartado 2.6.2 de la Guía.

<sup>101</sup> Las matrices RACI (*Responsible, Accountable, Consulted, Informed*) son un ejemplo de esta metodología para la toma de decisiones participada que utiliza ISO en todas sus recomendaciones pero que, sin embargo, son desconocidas en el planteamiento expresado en la norma española. Por su parte, la Guía AVAF sí que recoge este principio cuando reconoce la importancia de la escucha activa a la ciudadanía y la necesaria implicación de todos los actores en los procesos de toma de decisiones en sus apartados 2.6.5 y 2.6.6 de la Guía.

<sup>102</sup> El apartado 1 de la ISO 37002: objeto y campo de aplicación, afecta a las cuatro fases diferenciadas del ciclo de planificación y el control operacional de forma similar a las cuatro fases que experimentan las comunicaciones realizadas a través del canal externo de comunicaciones ante la Autoridad Independiente de Protección del Informante que se recogen en el Título III de la Ley 2/2023.

<sup>103</sup> El apartado 7.2 de la ISO 37002 se refiere a las características de fiabilidad, inteligencia emocional, diplomacia, imparcialidad, integridad, liderazgo, confidencialidad y buen juicio, que deben presentar los responsables de la protección, apoyo e investigación en el sistema de gestión de denuncias.

La norma española dedica un artículo al régimen de personal de la autoridad independiente, el artículo 45, con referencia a los principios que deben inspirar su proceso de selección y a la formación específica que deben recibir una vez incorporados.

Desde la Agencia Valenciana Antifraude animan a todas las entidades a designar un responsable de integridad que asumirá las funciones vinculadas a los canales internos de información pero también todas aquellas que requiera la ejecución del plan de integridad institucional y/o de cada uno de los marcos de integridad que impone la vigente legislación en materia de transparencia y buen gobierno, tales como: códigos éticos, procedimientos de prevención o control de los conflictos de interés, formación, como recogen las recomendaciones para la aplicación de la Ley 2/2023 en las entidades valencianas obligadas.

<sup>104</sup> El apartado 7.1 de la ISO 37002 hace referencia a los recursos necesarios (financieros y humanos, soluciones de TI, habilidades especializadas, infraestructura organizacional, material y experiencia) que deben integrar el apoyo de la organización.

De forma tangencial, el artículo 8.4 de la ley de protección del informante se refiere a que el responsable del sistema deberá disponer de todos los medios personales y materiales para llevar a cabo sus tareas frente a la adecuada dotación de recursos humanos que señala la Guía AVAF en su apartado 2.6.1. como aspecto fundamental dentro de todo plan de integridad pública que se quiera poner en marcha.

<sup>105</sup> Aunque debemos recordar que la función de gestión puede delegarse, en su totalidad o en parte, en personas externas a la organización siempre que su actividad sea susceptible de control y seguimiento por los responsables tal y como recoge el apartado 5.3.3 de la ISO 37002: características de la toma de decisiones delegada y de su control y permite el artículo 15 de la ley de protección del informante para las entidades que integran la Administración Local siempre que acrediten insuficiencia de medios y solamente con carácter instrumental.

Con respecto a la gestión indirecta del sistema interno de información por un tercero, desde la AVAF advierten que, en todo caso, su control debe residenciarse en el ámbito interno de la organización. La externalización, previa



proceso trazable y auditable, previamente aprobado, que garantice un trato imparcial y objetivo, en el que se identifique cómo se recibe la información, de qué manera se evalúa, qué medidas de protección se adoptan y para quién y qué recomendaciones o decisiones deben adoptarse al respecto una vez concluida la investigación, resultan esenciales<sup>106</sup>.

El canal de denuncias debe generar, además, incentivos suficientes para que la comunicación de las informaciones que pueden suponer riesgos para la organización se realice de forma segura. La alta dirección debe asegurar que, en las diferentes fases del procedimiento, se garantiza la protección del denunciante frente a posibles represalias a través del tratamiento confidencial de su identidad, la protección de datos personales y la puesta a disposición de medidas específicas de apoyo pero también la de los investigados frente a los comportamientos de mala fe que puedan desvirtuar el modelo<sup>107</sup>. El uso de una herramienta de software que garantice todas estas condiciones es esencial para el buen funcionamiento del canal de denuncias.

## 7. Documentación de los datos y de los resultados

La información generada por el canal de denuncias debe documentarse y controlarse en todas las fases del procedimiento, estar disponible de forma idónea para su uso, protegerse y conservarse y garantizar su tratamiento confidencial para evitar identificaciones que puedan desalentar las comunicaciones al mismo tiempo que permita la retroalimentación a las partes implicadas.

A pesar de estas cautelas, el denunciante tiene derecho a recibir comunicaciones del resultado de la investigación y de cualquier circunstancia relevante durante el procedimiento<sup>108</sup>.

---

justificación de la insuficiencia de medios propios, únicamente podría ser de carácter instrumental y sin que pueda implicar ejercicio de potestades públicas reservadas al personal funcionario de carrera en consonancia con el artículo 105 de la Constitución Española. Así aparece recogido en el apartado cuarto de la Guía para la implementación de la Ley 2/2023.

<sup>106</sup> El apartado 6.1 de la ISO 37002 se refiere a la responsabilidad de diseñar estos procesos de tratamiento y gestión de la información recibida y el apartado 8.1 recoge los pasos operativos del sistema de gestión. De forma bastante superficial, el artículo 9 de la ley de protección del informante recoge el contenido mínimo del procedimiento de gestión de informaciones pero no especifica o detalla cómo se deben llevar a cabo tales indicaciones.

La AVAF, en su Guía para la implementación de la Ley 2/2023, apartado séptimo, considera que las entidades del sector público deban velar por la implementación de todas las garantías y mecanismos necesarios para que en el procedimiento de recepción de informaciones sobre infracciones se puedan detectar eventuales posibles conflictos de interés entre el tercero y las personas informantes, prevenir y contener los riesgos de fuga de información institucional y los e o garantizar la protección de datos personales de las personas informantes, a título de ejemplo.

<sup>107</sup> El apartado 8.4 de la ISO 37002 recoge los instrumentos utilizados habitualmente en el tratamiento de las denuncias de irregularidades desde la protección y apoyo al denunciante, el tratamiento de la conducta perjudicial detectada, la protección de los sujetos de denuncia y de las partes interesadas pertinentes.

Por su parte, la norma española hace referencia en su artículo 5.2b) a la garantía de seguridad en el diseño de los sistemas internos de información, con independencia de su fórmula de gestión y en su artículo 17.3 al sistema de registro seguro y de acceso restringido que debe utilizarse en la fase de recepción de las informaciones. En lo referente tanto el canal interno como externo de comunicaciones, el artículo 26 recoge las obligaciones de registro de las informaciones recibidas e investigaciones realizadas garantizando los requisitos de confidencialidades previstos en la ley y el artículo 33 las relacionadas con la protección de datos.

La AVAF manifiesta en su Guía para la aplicación de la Ley 2/2023 que “la configuración del sistema interno de información debe reunir determinados requisitos, entre otros, su uso asequible, las garantías de confidencialidad, las prácticas correctas de seguimiento, investigación y protección del informante” y destaca que se permite la comunicación anónima ofreciendo el uso gratuito del software libre de gestión que utiliza la Agencia para sus buzones de denuncias, al tratarse de tecnologías que cumplen todos los requisitos requeridos por la Ley 2/2023 para el canal interno de información. Además, podemos referirnos a los dos sistemas de buzones digitales más conocidos y ampliamente utilizados como son *GlobalLeaks* —desarrollado por el Centro Hermes para la Transparencia y los Derechos Humanos y adaptado por AVAF para su canal de denuncias de irregularidades— y el sistema *SecureDrop* de la Fundación para la Libertad de Prensa.

<sup>108</sup> El nivel de detalle proporcionado al denunciante sobre las acciones tomadas por la organización puede, no obstante, verse limitado para evitar comprometer cualquier investigación según recoge el apartado 8.1 de la ISO 37002.

En diferentes apartados de la norma española, como en el artículo 9.2.c), se recogen las obligaciones de información al denunciante en el marco del sistema interno de información y en el artículo 17.4, 18.2, 19.2, 20.3 del título III cuando se tramitan comunicaciones ante el canal externo, todo ello en cumplimiento de las indicaciones de la Directiva *whistleblower*.

## 8. Medición y rendición de cuentas

La evaluación del desempeño del canal de denuncias es una parte esencial del sistema de gestión y, con el objetivo de analizar su eficacia, corresponde a las entidades la planificación de cómo, cuándo y por quién se va a realizar la medición y el análisis de sus resultados<sup>109</sup>.

La selección de un conjunto de indicadores, cuantitativos y cualitativos, que guíen estas tareas de seguimiento y evaluación, así como el desarrollo de auditorías internas planificadas permitirán comparar el desempeño del sistema de gestión de denuncias en diferentes periodos, fases y resultados<sup>110</sup>.

## 9. Revisión periódica y mejora continua

El canal de denuncias debe revisarse de forma periódica a través del análisis de los resultados obtenidos, las necesidades y expectativas generadas, los cambios de contexto que se hayan podido producir y las oportunidades surgidas de la práctica. Los resultados de este proceso de revisión y los datos estadísticos generados del análisis propician la actualización, verificación puntual y sobrevenida y la mejora del sistema<sup>111</sup>.

Los estándares sobre gestión de denuncias de irregularidades exigen la mejora continua de estos canales. Esta actividad debe realizarse de forma planificada por el órgano de gobierno y a propuesta de la alta dirección, periódicamente y, en todo caso, cuando se haya detectado una necesidad que afecte a la idoneidad, adecuación o eficacia del sistema de gestión<sup>112</sup>.

## V. CONCLUSIONES

Mejorar la cultura ética y de integridad y reforzar los vínculos existentes con la ciudadanía se plantean como prioridades de la gestión pública contemporánea. La incorporación de nuevos enfoques procedentes de las ciencias sociales, unido al poder transformador de la tecnología, aparecen como revulsivos para la consolidación de una gestión de los asuntos públicos más inteligente, responsable y transparente.

Los canales de denuncias en el ámbito público se presentan como una oportunidad para la promoción de ambos objetivos. Por un lado, permiten un mejor uso de la información disponible

---

<sup>109</sup> El apartado 6.2 de la ISO 37002 hace referencia a que los objetivos del sistema de gestión de denuncia de irregularidades deben ser medibles, objeto de seguimiento y evaluación y ser actualizados o revisados según los casos.

En la Disposición Adicional tercera de la Ley de protección del informante se recoge la obligación de elaborar una memoria anual en los tres primeros meses del año de la que se dará cuenta de las actuaciones desarrolladas durante el año anterior pero sin embargo no prevé esta obligación de rendición de cuentas para las entidades obligadas a implantar canales internos de informaciones.

Por su parte, la AVAF da cuenta de todas sus actuaciones y realiza un seguimiento de las mismas, las resoluciones finales de investigación son publicadas en la web y anualmente acude a las Cortes a presentar su memoria anual o, en el caso que así proceda, el informe extraordinario que se eleva a la comisión parlamentaria correspondiente.

<sup>110</sup> El apartado 9.1.2 de la ISO 37002 recoge un listado no exhaustivo de indicadores que pueden ser utilizados con estos fines como, por ejemplo, el número de denuncias recibidas por país, región y departamento, la naturaleza de la irregularidad, el tiempo de acoso de recibo de la denuncia inicial de irregularidades o la proporción de denuncias que quedan fuera del alcance del Sistema o aquellas en que la Información era deliberadamente falsa. En el mismo sentido, encontramos el Anexo IX de la Guía AVAF: El Plan de integridad pública.

<sup>111</sup> El apartado 9.3 de la ISO 37002 se refiere a la revisión que debe realizarse y trasladarse al órgano de gobierno para la adopción de decisiones mientras que la norma española prevé, en su artículo 22, que cada tres años se revisará y modificará el procedimiento de gestión de informaciones de la autoridad independiente para su mejora continua.

El plan de integridad, y dentro del mismo el canal de denuncias, debe configurarse como una herramienta flexible y sujeta a revisión y actualización, según el apartado 2.11 de la Guía AVAF por lo que se recomienda definir con claridad y precisión el procedimiento y órgano que lo impulse.

<sup>112</sup> La ISO 37002 hace referencia, cuando habla de mejoras continuas, a la reacción de la organización en caso de “no conformidades” entendidas como aquellos supuestos en los que se constata el incumplimiento de un requisito y la necesidad de incorporar acciones correctivas o mecanismos para eliminar el origen del incumplimiento y prevenir la recurrencia, cuando la normativa española establece la revisión de los procedimientos al menos una vez cada 3 años.

facilitada por las personas directamente vinculadas al caso concreto mitigando así los problemas de información en la toma de decisiones y, por otro, fomentan la participación directa de la ciudadanía en la identificación de los riesgos y las reacciones ante los incumplimientos colaborando, como actores principales, en la construcción de una cultura de cumplimiento de la organización.

A pesar de que la implantación de canales de denuncias, en su denominación más general, o de sistemas internos de información, canales internos o canales externos de información en la denominación particular por la que ha optado el legislador español, es preceptiva para todo el sector público a partir de la transposición a nuestro ordenamiento jurídico de la Directiva *whistleblower* y que los fondos MRR han otorgado cierta relevancia a los aspectos éticos en las entidades que gestionan fondos públicos, las omisiones, incoherencias y los defectos de técnica de la nueva normativa nos han animado a trabajar en una guía, en forma de principios generales de aplicación, al servicio de las administraciones públicas.

Organizaciones dedicadas a la lucha contra el fraude de ámbito municipal, regional, estatal o europeo, atesoran una vasta experiencia en la gestión de canales de denuncias y sus contribuciones, advertencias y recomendaciones son especialmente interesantes en esta tarea. Del mismo modo, en el sector privado, desde la reforma del Código Penal del año 2015 las empresas han estado trabajando en la puesta en marcha de mecanismos para evitar o reducir la responsabilidad penal en la que pudieran incurrir sus organizaciones y sus mejores prácticas en materia de canales de denuncias se ven recopiladas en las normas técnicas ISO de alcance internacional.

Un análisis cuidadoso y reflexivo del marco teórico indicado y de las mejores prácticas del sector público y privado a partir de las dos experiencias citadas llevan a proponer en este trabajo un catálogo de nueve principios generales de aplicación que, pensamos, puede servir de guía a las administraciones públicas en su tarea de diseñar e implementar canales de denuncias que cumplan de manera eficaz su cometido: la implicación y compromiso al más alto nivel; la integración del canal de denuncias en la política de integridad; la determinación de los riesgos y definición del alcance de la protección; la publicidad, difusión y participación; la suficiencia de recursos; el tratamiento seguro de la información; la documentación de los datos y de los resultados; la medición y rendición de cuentas y la revisión periódica y mejora continua.

En definitiva, las administraciones públicas deben estar comprometidas con la implantación de una política de integridad real y efectiva, a medida de los riesgos de sus actividades y que cuente con herramientas, como los canales de denuncias, para su identificación y reacción. Además, deben poder demostrar este compromiso con la implicación directa de la cúpula de cada entidad en la aprobación del sistema, la designación de responsabilidades y la garantía de medios técnicos seguros y humanos suficientes para llevar a cabo su implementación. Y, en última instancia, deben saber comunicar, tanto dentro como fuera de cada entidad, los resultados de esta implicación a través de la publicidad y difusión del sistema y de sus logros, la adecuada formación de todo su personal y la evaluación y actualización de su funcionamiento.

## VI. BIBLIOGRAFÍA

- ALOISI, A., DE STEFANO, V. (2022): *Your boss is an algorithm. Artificial Intelligence, Platform Work and Labour*. London: Hart.
- ARÁNGUEZ SÁNCHEZ, C. (2020): “El diseño de programas de prevención de delitos para personas jurídicas”. *Revista Electrónica de Ciencia Penal y Criminología*, n.º 22-20.
- ARENILLA SÁEZ, M. (2014): *Teclas para transformar la Administración Pública española. Grupo de Investigación en Administración Pública 2032*. Madrid: INAP [<http://www.gigapp.org/images/stories/Teclas-GLAP2032-V1-1.pdf>].
- ARES GONZÁLEZ, B. (2021): “El Estatuto del denunciante y el canal de denuncias en el ámbito público”. En: RODRÍGUEZ-GARCÍA, N., RODRÍGUEZ LÓPEZ, F. (eds.): *Compliance y responsabilidad de las personas jurídicas*. Valencia: Tirant lo Blanch.

- ASOCIACIÓN ESPAÑOLA DE COMPLIANCE (2020): *Estudio sobre la función de compliance en las empresas españolas*. Madrid: ASCOM.
- ATIENZA RODRÍGUEZ, M. (2006): *El Derecho como argumentación. Concepciones de la argumentación*. Barcelona: Ariel.
- AVAF (2023): *Guía para la aplicación de la Ley 2/2023, de 20 de febrero* [[https://www.antifraucv.es/wp-content/uploads/2023/03/GULA-AVAF-LEY-2\\_2023\\_.pdf](https://www.antifraucv.es/wp-content/uploads/2023/03/GULA-AVAF-LEY-2_2023_.pdf)].
- BACHMAIER WINTER, L. (2019): “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*, n.º 9539.
- BALLESTEROS SÁNCHEZ, J. (2020): “Pautas y recomendaciones técnico-jurídicas para la configuración de un canal de denuncias eficaz en organizaciones públicas y privadas. La perspectiva española”. *Derecho PUCP*, n.º 85.
- BARCELÓ MOYANO, M. (2023): “Obligaciones de reporte al Ministerio Fiscal en la nueva Ley de protección de whistleblowers”. *Actualidad Jurídica Uría Menéndez*, n.º 61.
- BECK, U. (1999): *World Risk Society*. Oxford: Policy Press.
- CAMPOS ACUÑA, C. (2017): “Encaje del SALER en el nuevo marco legal de lucha contra la corrupción: una herramienta de compliance”. *Revista Internacional de Transparencia e Integridad*, n.º 5.
- CAMPOS ACUÑA, C. (2020): “Guía práctica de compliance en el sector público”. *El Consultor de los Ayuntamientos*.
- CAMPOS ACUÑA, C. (2022): “Canales de denuncia y protección del denunciante en el ámbito local. Algunas dificultades propias de la administración local y propuestas de solución”. En: GIMENO BEVIÁ J., LÓPEZ DONAIRE, M. B. (dirs.): *La protección de denunciantes: Propuesta de regulación para España tras la Directiva Whistleblowing*. Valencia: Tirant lo Blanch.
- CAMPOS ACUÑA, C. (2023): “Las 15 claves del Sistema Interno de Información («Whistleblower»)””. *Carta Tributaria. Revista de Opinión*, n.º 95.
- CASANOVAS YSLA, A. (2017): *Compliance penal normalizado: el estándar UNE 19601*. Pamplona: Aranzadi.
- CASANOVAS YSLA, A. (2018): “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*. Pamplona: Thomson-Reuters Aranzadi.
- CASTAÑEDA CRESPO, C. E. (2022): “Public compliance”. En: RAMÍREZ BARBOSA, P. A. (dir.): *Responsabilidad empresarial y cumplimiento corporativo*. Bogotá: Tirant lo Blanch.
- CEREZO PRIETO, M., FRUTOS ESTEBAN, F. J. (2022): “Los nudges como herramienta al servicio de la gobernanza anticipatoria”. En: SÁNCHEZ SÁNCHEZ, Z. (dir.): *Regulación con prospectiva de futuro y de consenso gobernanza anticipatoria y prospectiva administrativa*. Pamplona: Aranzadi.
- COLVIN N., GALIZZI B., NAD, V. (2020): *Cómo proteger mejor a los alertadores: Guía práctica para transponer la Directiva europea* [<https://www.blueprintforfreespeech.net/es/noticias/guia-practica-para-la-transposicion-de-la-directiva-de-la-ue-sobre-los-alertadores>].
- COMISIÓN EUROPEA (2019): *The Innovation Principle, European Commission, Research and Innovation Department* [[https://research-and-innovation.ec.europa.eu/system/files/2022-07/ec\\_rtd\\_factsheet-innovation-principle.pdf](https://research-and-innovation.ec.europa.eu/system/files/2022-07/ec_rtd_factsheet-innovation-principle.pdf)].
- COMISIÓN EUROPEA (2022): *An EU Strategy on Standardisation Setting global standards in support of a resilient, green and digital EU single market* [<https://ec.europa.eu/docsroom/documents/48598/attachments/2/translations/en/renditions/native>].
- COMISIÓN EUROPEA (2022a): *Eurobarómetro especial sobre la corrupción* [<https://europa.eu/eurobarometer/surveys/detail/2658>].
- COMISIÓN EUROPEA (2022b): *Informe sobre el Estado de Derecho en 2022. La situación del Estado de Derecho en España* [[https://commission.europa.eu/publications/2022-rule-law-report-communication-and-country-chapters\\_en](https://commission.europa.eu/publications/2022-rule-law-report-communication-and-country-chapters_en)].



- COMITÉ ECONÓMICO Y SOCIAL EUROPEO (2017): *Dictamen sobre «Integrar los nudges en las políticas europeas»* [<https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52016IE1333>].
- CRIADO GRANDE, J. I. (2016): “Las administraciones públicas en la era del gobierno abierto. Gobernanza inteligente para un cambio de paradigma en la gestión pública”. *Revista de Estudios Políticos*.
- DÍAZ MÉNDEZ, A., CUÉLLAR MARTÍN, E. (2007): *Gestión pública inteligente*. Madrid: Ministerio de Administraciones Públicas.
- DOMÉNECH PASCUAL, G. (2022): “Las regulaciones experimentales”. *Anuario del Buen Gobierno y de la Calidad de la Regulación*.
- DUPUY K., NESET, S. (2020): *La psicología cognitiva de la corrupción. Explicaciones del comportamiento no ético a nivel micro*. Oslo: CMI.
- FERNÁNDEZ AJENJO, J. A. (2019): “Problemas y soluciones frente al uso populista del Estado de Derecho: Agencias Anticorrupción y Servicios de Coordinación Antifraude”. *Revista Internacional de Transparencia e Integridad*.
- FERNÁNDEZ AJENJO, J. A. (2020): “Comentarios a la Directiva UE 2019/1937 relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión”. En: RODRÍGUEZ-GARCÍA, N., RODRÍGUEZ LÓPEZ, F. (eds.): *Compliance y justicia colaborativa en la prevención de la corrupción*. Valencia: Tirant lo Blanch.
- FERNÁNDEZ AJENJO, J. A. (2022): *Instituciones de investigación administrativa y auditoría forense para la prevención del fraude y la corrupción en las Administraciones Públicas*. Valencia: Tirant lo Blanch.
- FORTUNY, M. (2020): “La nueva guía DOJ para evaluar la eficacia de un programa de cumplimiento: un horizonte de legitimidad más allá del *paper compliance*”. *La Ley Compliance Penal*, n.º 2.
- GALÁN MUÑOZ, A. (2019): “*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.
- GAMERO CASADO, E. (2021): “*Compliance* (o cumplimiento normativo) de desarrollos de Inteligencia Artificial para la toma de decisiones administrativas”. *Diario La Ley*, n.º 50.
- GARCÍA MORENO, B. (2020): *Del whistleblower al alertador. La regulación europea de los canales de denuncia*. Valencia: Tirant lo Blanch.
- GARCÍA MORENO, B. (2021): “El concepto de alertador (o *whistleblower*). Consideraciones a la luz de la Directiva (UE) 2019/1937”. En: RODRÍGUEZ-GARCÍA, N., RODRÍGUEZ LÓPEZ, F. (coords.), *Compliance y responsabilidad de las personas jurídicas*. Valencia: Tirant lo Blanch.
- GARCÍA MORENO, B. (2022): “La figura del *whistleblower*”. En: LÓPEZ DONAIRE, B., GIMENO BEVIÁ, J. (dirs.): *La directiva de protección de los denunciantes y su aplicación práctica al sector público*. Valencia: Tirant lo Blanch.
- GIMENO BEVIÁ, J. (2021): “*Whistleblowing* y proceso penal: una lectura desde las garantías procesales”. En: OLAIZOLA NOGALES, I., SIERRA HERNÁIZ, E., 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.
- GIMENO FELIÚ, J. M. (2022): “Los fondos *Next Generation* y el rol de los órganos de control externo. Auditoría y control de la respuesta al Covid-19 y de la implementación de la iniciativa *Next Generation UE*”. En: VV.AA.: *XIV Encuentros Técnicos de los OCEX*. Santiago de Compostela: Thomson-Reuters Aranzadi.
- GOÑI SEIN, J. L. (2021): “Canal de denuncias en la empresa y protección de datos”. En: OLAIZOLA NOGALES, I., SIERRA HERNÁIZ, E., 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.
- GUTIÉRREZ RODRÍGUEZ, M. (2022): “Las normas UNE-ISO y su referencia a los canales de denuncia”. En: GIMENO BEVIÁ J., LÓPEZ DONAIRE, M. B. (dirs.): *La protección de denunciantes: Propuesta de regulación para España tras la Directiva Whistleblowing*. Valencia: Tirant lo Blanch.
- HEREDERO ORTIZ DE LA TABLA, L. (2022): “La construcción de un sistema de integridad institucional en la Administración de Castilla y León (2007-2021)”. *Revista Gestión y Análisis de Políticas Públicas (GAPP)*, n.º 28.
- IGLESIAS REY, P. (2022): “El desafío del sector público ante la aplicación de la Directiva de protección del informante. Los canales de denuncia”. *Revista Galega de Administración Pública (EGAP)*, n.º 64.
- IGLESIAS REY, P. (2023): “Implicaciones de la nueva ley de protección del informante: la exigencia de los canales de denuncia en el sector público como un elemento nuclear de los sistemas de integridad”. *Revista Auditoría Pública*, n.º 81.
- JIMÉNEZ ASENSIO, R. (2022): “Integridad pública y prevención. A propósito del diseño y aplicación de las medidas de prevención en los planes antifraude en la gestión de fondos europeos”. En: VV.AA.: *XIV Encuentros Técnicos de los OCEX*. Santiago de Compostela: Thomson-Reuters Aranzadi.
- JIMÉNEZ FRANCO, E. (2022): “Prospectiva administrativa y la futura Ley de protección de los informantes”. En: SÁNCHEZ SÁNCHEZ, Z. (dir.): *Regulación con prospectiva de futuro y de consenso gubernanza anticipatoria y prospectiva administrativa*. Cizur Menor: Aranzadi.
- KAHNEMAN, D. (2011): *Thinking, Fast and Slow*. London: Penguin Books.
- KAHNEMAN, D., SLOVIC, P., TVERSKY, A. (eds.) (1982): *Judgment under uncertainty: Heuristics and biases*. Cambridge: Cambridge University Press
- LEO CASTELA, J. I., RODRÍGUEZ LÓPEZ, F., SÁNCHEZ MACÍAS, J. I. (2019): “Evolución de la responsabilidad social y legal corporativa: hacia un índice de *compliance* en la OCDE”. En: RODRÍGUEZ-GARCÍA, N., CARRIZO GONZÁLEZ CASTELL, A., RODRÍGUEZ LÓPEZ, F. (eds.): *Corrupción: compliance, represión y recuperación de activos*. Valencia: Tirant lo Blanch.
- LEÓN ALAPONT, J. (2020): *Compliance penal. Especial referencia a los partidos políticos*. Valencia: Tirant lo Blanch.
- LEÓN ALAPONT, J. (2022): “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”. *UNED. Revista de Derecho Penal y Criminología*, n.º 28.
- LEÓN ALAPONT, J. (2023): *Canales de denuncia e investigaciones internas en el marco del compliance penal corporativo*. Valencia: Tirant lo Blanch.
- LÓPEZ DONAIRE, M. B. (2022): “Marcos de integridad y los canales de denuncia. El derecho a la buena administración”. En: GIMENO BEVIÁ J., LÓPEZ DONAIRE, M. B. (dir.): *La protección de denunciantes: propuesta de regulación para España tras la Directiva Whistleblowing*. Valencia: Tirant lo Blanch.
- MAGRO SERVET, V. (2020): “¿Por qué es recomendable un canal de denuncias interno en la empresa?”. *Diario La Ley*, n.º 9586.
- MAGRO SERVET, V. (2023): “Denuncia anónima, el confidente, el canal de denuncias y la Ley 2/2023 de 20 de febrero de protección del «alertador» ante la corrupción”. *Diario La Ley*, n.º 10239.
- MINSAIT (2021): *Boosting Intelligence Governance: la gestión pública del mañana*. Madrid: INDRA [<https://www.minsait.com/es/actualidad/insights/las-claves-del-gobierno-inteligente-en-las-administraciones-publicas>].
- MONTANER FERNÁNDEZ, R. (2018): “La exención de responsabilidad penal de las personas jurídicas: Regulación jurídico-penal vs. UNE 19601”. *La Ley Penal*, n.º 132.

- MUNDORF, S., VILLAREJO GALENDE, H. (2015): “El interés público y la supervisión de la auditoría. ¿Cómo debe vigilar el vigilante?”. *AECA: Revista de la Asociación Española de Contabilidad y Administración de Empresas*, vol. 111.
- MUÑOZ JUNCOSA, A. (2023): “La influencia del modelo de control interno de la UE en el control de los fondos *Next Generation*”. *El consultor de los Ayuntamientos y de los Juzgados*, n.º 3.
- OCDE (2018) *La integridad pública desde una perspectiva conductual. El factor humano como herramienta anticorrupción*. Paris: OCDE [<https://www.oecd.org/publications/la-integridad-publica-desde-una-perspectiva-conductual-9789264306745-es.htm>].
- PÉREZ TRIVIÑO, J. L. (2018): “Los canales de denuncia en las organizaciones deportivas. Un análisis pesimista”. *Revista Internacional de Transparencia e Integridad*, n.º 8.
- PONCE SOLÉ, J. (2018): “Derecho administrativo, ciencias conductuales y *nudging* en la gestión pública”. *Revista Vasca de Gestión de Personas y Organizaciones Públicas*, n.º 15.
- PWC (2012): *¿En qué hay que transformar la Administración Pública española? Como afrontar el reto del cambio en el sector público*. Madrid: PwC [<https://www.pwc.es/es/publicaciones/sector-publico/assets/transformar-administracion-publica-esp.pdf>].
- PWC (2020): *Administración 2030: Una visión transformadora. Propuestas para la próxima década*. Madrid: PwC [<https://www.pwc.es/es/publicaciones/sector-publico/assets/observatorio-pwc-esade-administracion-2030.pdf>].
- RAGÜES I VALLÉS, R. (2021): “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*, n.º 7.
- RIVERO ORTEGA, R. (2007). *Derecho Administrativo económico*. Madrid: Marcial Pons.
- RIVERO ORTEGA, R. (2017): “Gestión pública inteligente, innovación e información: oportunidades y riesgos del *big data* administrativo”. En: FERNANDO PABLO, M. M., FERNÁNDEZ DE GATTA SÁNCHEZ, D., RIVERO ORTEGA, R., TERRÓN SANTOS, D. (eds.): *Liber Amicorum Salmanticensis Profesor Ángel Sánchez Blanco (cuarenta años de ordenamiento constitucional)*. Salamanca: Ratio Legis.
- RIVERO ORTEGA, R. (2021): “La controvertida gestión de los fondos de recuperación en España: exigencias europeas y consenso futuro”. *REDE: Revista Española de Derecho Europeo*, n.º 80.
- RIVERO ORTEGA, R. (2022a): “La Administración del futuro: Gobierno de la prevision”. En: SÁNCHEZ SÁNCHEZ, Z. (dir.): *Regulación con prospectiva de futuro y de consenso gobernanza anticipatoria y prospectiva administrativa*. Cizur Menor: Thomson-Reuters Aranzadi.
- RIVERO ORTEGA, R. (2022b): “¿Cumplen el Derecho Europeo y Estatal las normas autonómicas sobre la gestión de los Fondos de Recuperación?”. *Revista Aragonesa de Administración Pública*, n.º 58.
- RODRÍGUEZ LÓPEZ, F. (2000): “Introducción al análisis económico de la corrupción”. En: FABIÁN CAPARRÓS, E. A. (ed.): *La corrupción: aspectos jurídicos y económicos*. Salamanca: Ratio Legis.
- RODRÍGUEZ LÓPEZ, F., SÁNCHEZ MACÍAS, J. I. (2021): “Normalización y certificación en *compliance*, de la autorregulación al valor social”. En: RODRÍGUEZ-GARCÍA, N., RODRÍGUEZ LÓPEZ, F. (eds): *Compliance y responsabilidad de las personas jurídicas*. Valencia: Tirant lo Blanch.
- RODRÍGUEZ-GARCÍA, N. (2023): “*Compliance* y sistema penal español: potencialidades y retos”. En: ARANGÜENA FANEGO, C., HOYOS SANCHO, M., PILLADO GONZÁLEZ, E., FREITAS, P. M. (eds.): *El proceso penal ante una nueva realidad tecnológica europea*. Cizur Menor: Thomson-Reuters Aranzadi.
- SÁEZ HIDALGO, I. (2022): “Claves para la implantación en el sector público de los canales de denuncias internas”. *Actualidad Administrativa*, n.º 5.

- SÁEZ HIDALGO, I. (2023): “El ámbito objetivo de aplicación de la Ley 2/2023. ¿Qué comunicaciones pueden justificar el derecho a protección frente a las represalias?”. *Diario La Ley*, n.º 10274.
- SÁNCHEZ MACÍAS, J. I., LEO CASTELA, J. I. (2020): *Compliance tributario para pymes según la Norma UNE 19602*. Madrid: AENOR Ediciones.
- SÁNCHEZ MACÍAS, J. I., RODRÍGUEZ LÓPEZ, F. (2021): “Estudio preliminar”. En: RODRÍGUEZ-GARCÍA, N. (dir.): *Tratado angloiberoamericano sobre compliance penal*. Valencia: Tirant lo Blanch.
- SÁNCHEZ SÁNCHEZ R. M. (2020): “Sistemas de *compliance* y canales de denuncia en la Administración Pública. Una referencia al Ayuntamiento de Barcelona y a su buzón ético y de buen gobierno”. *La Ley Compliance Penal*, n.º 2.
- SÁNCHEZ SÁNCHEZ, Z. (dir.) (2022): *Regulación con prospectiva de futuro y de consenso. Gobernanza anticipatoria y prospectiva administrativa*. Cizur Menor: Aranzadi.
- SENDÍN GARCÍA, M. A. (2019) “Régimen jurídico de la denuncia, indefensión del denunciante e interpretación del derecho por la Administración pública”. *Revista Galega de Administración Pública (REGAP)*, n.º 57.
- STIGLITZ, J. E. (2002): “Information and the Change in the Paradigm in Economics”. *American Economic Review*, vol. 92, n.º 3.
- TERRÓN SANTOS, D. (2021): “Reformas institucionales para la ejecución de los Fondos *Next Generation EU*”. En: RASTROLLO SUÁREZ, J. (dir): *Guía para la planificación, gestión y ejecución de los fondos del Plan para la Recuperación Transformación y Resiliencia*. Cizur Menor: Thomson-Reuters Aranzadi.
- THALER, R. H., SUNSTEIN, C. R. (2008): *Nudge: Improving Decisions about Health, Wealth and Happiness*. Yale: Yale University Press.
- THÜSING G., FORST, G. (2015): *Whistleblowing. A Comparative Study*. New York: Springer.
- TRANSPARENCIA INTERNACIONAL (2023): *Índice de Percepción de la Corrupción (IPC) 2022* [<https://www.transparency.org/en/cpi/2022>].
- TRANSPARENCY INTERNATIONAL (2018): *A Best Practice Guide for Whistleblowing Legislation* [<https://www.transparency.org/en/publications/best-practice-guide-for-whistleblowing-legislation>].
- U.S. DEPARTMENT OF JUSTICE CRIMINAL DIVISION (2020): *Evaluation of Corporate Compliance Programs* [<https://www.justice.gov/criminal-fraud/page/file/937501/download>].
- VEIGA MAREQUE, J. A., FERNANDEZ DE AVILÉS, G. (2019): *Compliance para pymes. Paso a paso*. Madrid: Colex.
- VILLEGAS GARCÍA, M. A., ENCINAR DEL POZO, M. A. (2018): “*Compliance*, protección del informante e investigaciones internas”. En: GÓMEZ JARA DIEZ, C. (coord.): *Persuadir y razonar: Estudios Jurídicos en homenaje a José Manuel Maza Martín*. Pamplona: Thomson-Reuters Aranzadi.
- VILLORIA MENDIETA, M. (2020): *Ética pública y corrupción: Curso de ética administrativa*. Madrid: Tecnos.
- WHISTLEBLOWING INTERNATIONAL NETWORK (WIN) (2023): *Carta dirigida a la Comisión Europea* [<https://es.scribd.com/document/624367047/25-01-23-WIN-Letter-EC-Re-Spain-Transposition-fin#>].
- XNET (2023): *Urgente: Enmiendas al Anteproyecto de Ley de Protección de Informantes/Alertadores/Whistleblowers, de 17 de marzo de 2022*. Barcelona: Xnet [<https://xnet-x.net/es/xnet-enmendar-anteproyecto-ley-proteccion-informantes-ministerio-justicia/>].