Grant Thornton

Ir a la web

Compliance Advisory LAB

Investigación sobre Compliance, *Forensic* y R.P.P.J. de Grant Thornton

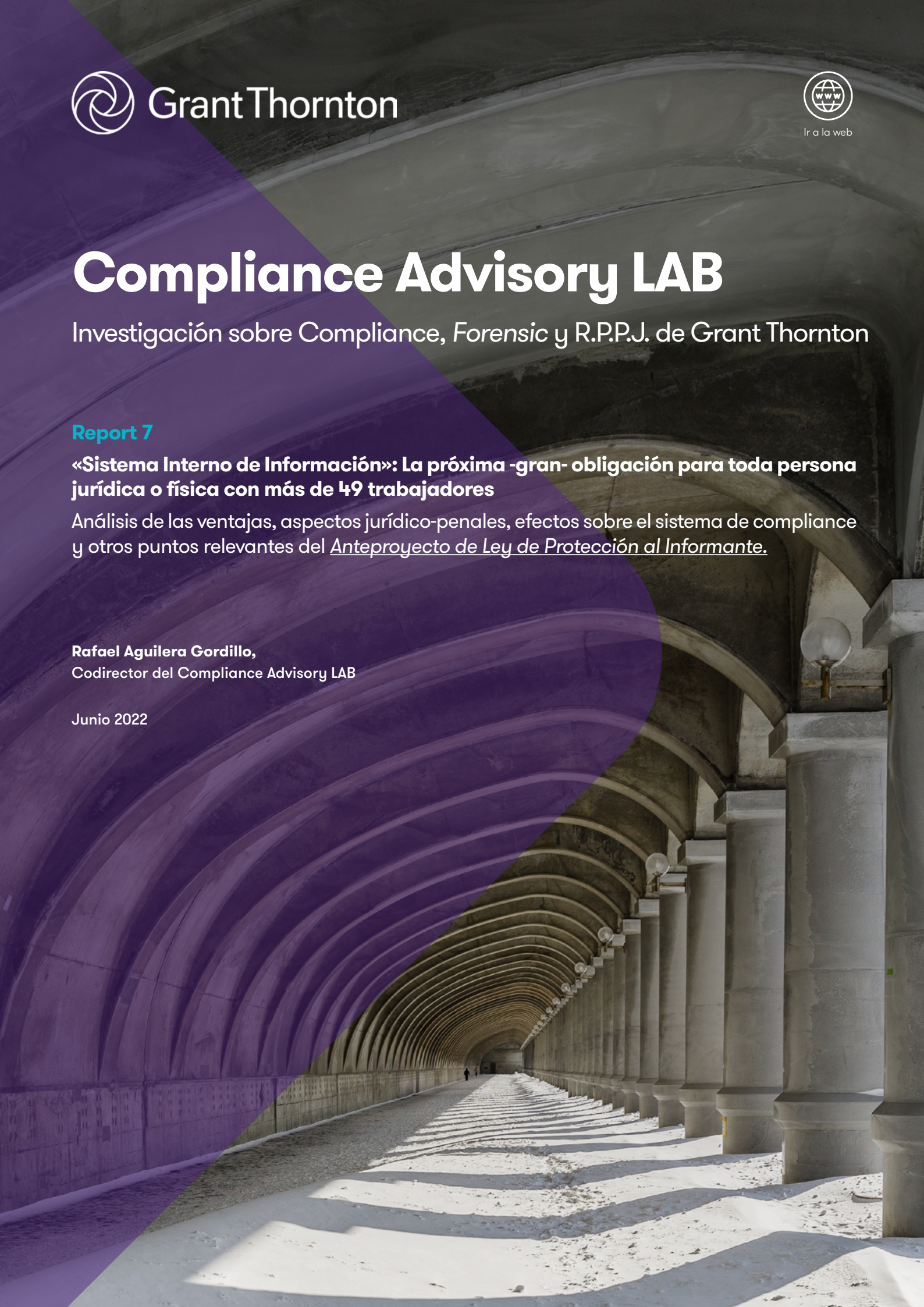
Report 7

«Sistema Interno de Información»: La próxima -gran- obligación para toda persona jurídica o física con más de 49 trabajadores

Análisis de las ventajas, aspectos jurídico-penales, efectos sobre el sistema de compliance y otros puntos relevantes del *Anteproyecto de Ley de Protección al Informante.*

Rafael Aguilera Gordillo,
Codirector del Compliance Advisory LAB

Junio 2022



Report 7

«Sistema Interno de Información»: La próxima -gran- obligación para toda persona jurídica o física con más de 49 trabajadores.

Análisis de las ventajas, aspectos jurídico-penales, efectos sobre el sistema de compliance y otros puntos relevantes del *Anteproyecto de Ley de Protección al Informante.*

La transposición al ordenamiento jurídico español de la Directiva «whistleblowing»[1] es, desde hace meses, una asignatura pendiente para las autoridades españolas. Como resulta conocido, esta Directiva obliga a los Estados miembros a aprobar disposiciones legales que impongan, a los agentes de los sectores privado y público el establecimiento de un sistema de denuncias y el despliegue de mecanismos que garanticen la protección al informante de infracciones del Derecho de la Unión[2].

El período para transponer la Directiva al ordenamiento jurídico nacional concluyó el 17 de diciembre de 2021. Este retraso ha originado, precisamente, que la Comisión Europea activara el procedimiento de infracción contra España[3] y otros países incumplidores[4]. **Sin embargo, la aprobación el pasado mes de marzo -por parte del Gobierno- del *Anteproyecto de Ley para proteger a las personas que informen sobre infracciones normativas corrupción y de lucha contra la corrupción*[5] (en adelante, Anteproyecto de Ley de Protección al Informante), parece ser el principio del fin de esta situación de impasse en que nos encontramos.**

Veremos cuánto se tarda en presentar y tramitar como «proyecto de Ley» en las Cortes, pero no cabe duda de que esta norma (que profundiza y amplía las exigencias previstas en la Directiva «whistleblowing») **va a generar, irremediablemente, un importantísimo cambio de paradigma en la gestión de riesgos de las corporaciones españolas,** en su diseño institucional y en el modo de afrontar la recepción y tramitación de avisos sobre posibles irregularidades cometidas en el seno de las mismas.

1. Término con el que, habitualmente, se conoce 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. Disponible en: https://www.boe.es/doue/2019/305/L00017-00056.pdf

2. Entes del sector privado de más de cincuenta trabajadores (Art. 8.3). Infracciones que engloban: contratación pública; servicios, productos y mercados financieros, y prevención del blanqueo de capitales y la financiación del terrorismo; seguridad de los productos y conformidad; seguridad del transporte; protección del medio ambiente; protección frente a las radiaciones y seguridad nuclear; seguridad de los alimentos y los piensos, sanidad animal y bienestar de los animales; salud pública; protección de los consumidores; protección de la privacidad y de los datos personales, y seguridad de las redes y los sistemas de información; infracciones que afecten a los intereses financieros de la Unión; infracciones relativas al mercado interior… (Art.2). No obstante, como podrá extraerse del presente análisis, el legislador español va más allá, extendiendo ámbito de aplicación material, personal y niveles de exigencia.

3. Decisión adoptada por la Comisión Europea el 27 de enero de 2022, procedimiento INFR(2022)0073. Disponible en: https://ec.europa.eu/atwork/applying-eu-law/infringements-proceedings/infringement_decisions/?lang_code=en. Italia, Hungría, Francia, Austria, Grecia o Bulgaria también se encontraban entre los países incumplidores contra los que se activó este tipo de procedimiento. La transposición resulta obligada.

4. Cuando la transposición de una directiva no se realiza -o se hace de manera incorrecta- y, dicha directiva, atribuye derechos concretos a los particulares, estos pueden alegarse ante los tribunales en virtud del «efecto directo» (vid. sentencia asunto C-91/92, Paola Faccini Dori contra Recreb Srl) y en determinadas condiciones pueden solicitar una «compensación» (vid. sentencia de los asuntos C-6/90 y C-9/90, Francovich y Bonifaci contra Italia).

5. Anteproyecto de Ley reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción por la que se transpone la Directiva (UE) 2019/1937 del Parlamento Europeo y del Consejo, de 23 de octubre de 2019, relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión. Disponible en: https://www.mjusticia.gob.es/es/AreaTematica/ActividadLegislativa/Documents/APL%20INFORMANTES%20TRaMITE%20AUDIENCIA%20E%20INFORMACIONn%20PuBLICA_0803.pdf

A este respecto, puede aseverarse que debido a los **extensos ámbitos** (material y personal) de aplicación de la norma, **entidades obligadas** a disponer de estos «sistemas internos de información» (empresarios y personas jurídicas que tengan contratados a más de 49 empleados, en el sector privado) y el elenco **obligaciones** recogidas en el texto, **una parte relevante de los agentes que conforman el tejido corporativo español deberán adoptar estos *sistemas de información* o de denuncias internos y contemplar *mecanismos de blindaje del informante.*** Y ello, no solo implica la necesidad de adoptar procedimientos y herramientas técnicas apropiadas, rediseñar organigramas o dotar de formación específica sobre «denuncias internas», sino que, en la práctica, **va a producir la generalización de las «investigaciones internas corporativas» dimanantes de la recepción de tales denuncias, así como del resto de actuaciones específicas orientadas a esclarecer posibles casos de fraude, corrupción, etc. en el seno de las organizaciones.**

Es probable -incluso recomendable- que este *Anteproyecto de Ley de Protección al Informante* aprobado por el Ejecutivo soporte algunas alteraciones de contenido durante su tramitación, pero la práctica nos muestra que, en proyectos de estas características (donde se abordan cuestiones específicas alejadas de intereses partidistas), las obligaciones recogidas en las leyes que finalmente resultan aprobadas son sustancialmente coincidentes con las recogidas en los anteproyectos. Por tanto, **dado el impacto que la aprobación de esta norma ocasionará en empresas y autónomos, asociaciones y fundaciones, cooperativas y resto del panorama corporativo español, se estima pertinente ofrecer un análisis de su contenido.**

Como el lector va a tener la oportunidad de observar, se trata de un **examen que abarca los principales aspectos y ventajas que ofrece la norma, pero que, además, incorpora otras cuestiones de enorme calado como las implicaciones jurídico-penales que el cumplimiento de esta norma generará,** su armonización con las exigencias del Código Penal sobre programas de prevención o «sistemas de compliance», la posible afectación a la «no autoincriminación» de la persona jurídica, etc. **Entendemos que, solo desde ese enfoque analítico integral, podrá obtenerse una imagen más fiel y nítida de los efectos que la aprobación de esta norma van a producir dentro de**

las organizaciones; pues el propósito del presente *report* del Compliance Advisory LAB de Grant Thornton es que sea considerado como un documento de utilidad para especialistas en Compliance y Penal Corporativo o para aquellos profesionales que, dadas las funciones que desempeñan dentro de una organización, puedan verse especialmente afectados por las disposiciones de la norma. Por tanto, **este séptimo report resulta de particular interés para compliance officers, asesores legales corporativos, analistas de riesgos, órganos colegiados con funciones vinculadas al compliance y, como veremos, para los futuros responsables del denominado «sistema de información interna».**

Asimismo, como podrá verse en la parte final del informe, **el incumplimiento de las exigencias que contiene la norma conllevará imposición de sanciones de gran envergadura para el empresario o persona jurídica**[6] (además, crea una «Autoridad Independiente de Protección al Informante» que velará por la debida observancia de tales exigencias, activando procedimiento sancionador cuando aprecie incumplimientos), **por lo que el objeto de este informe concierne tanto a directivos como a miembros del consejo de administración.**

Este Anteproyecto está conformado por sesenta y ocho artículos, tres disposiciones adicionales, cuatro transitorias y ocho disposiciones finales. Sus preceptos se estructuran en nueve títulos. No obstante, dado que la presente **evaluación de contenido del Anteproyecto de Ley de Protección al Informante se centra en la incidencia de la norma sobre empresarios, empresas y otros entes corporativos dentro del sector privado** (dejando en plano secundario a los aspectos íntimamente ligados al sector público), la estructura del análisis dotará de mayor protagonismo a los títulos que más incidencia tienen sobre el sector privado[7] y se refundirán aquellos particularmente vinculados al ámbito público.

6. A este respecto, cabe adelantar que el artículo 65 de este Anteproyecto de Ley de Protección al Informante contempla las siguientes multas y sanciones de otra naturaleza:

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

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

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

a) La amonestación pública. b) La prohibición de obtener subvenciones u otros beneficios fiscales durante un plazo máximo de cuatro años. c) La prohibición de contratar con el sector público durante un plazo máximo de tres años […].

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

7. Títulos que componen el Anteproyecto de Ley de Protección al Informante: TITULO I Finalidad de la ley y ámbito de aplicación; TÍTULO II Sistemas internos de información; TÍTULO III Canal externo de informaciones; TÍTULO IV Disposiciones comunes a los canales internos y externos; TITULO V Revelación pública; TITULO VI Protección de datos personales; TITULO VII Medidas de protección; TÍTULO VIII Autoridad Independiente de Protección del Informante y TÍTULO IX Régimen sancionador.

1. «Finalidad de la ley y ámbito de aplicación»

Aunque el objetivo inmediato de este *Anteproyecto de Ley de Protección al Informante* es **proteger a quienes alertan o denuncian de prácticas conductas ilegales,** el texto se incardina en la tendencia de los poderes públicos consistente en aprobar disposiciones que impulsen, en el seno de las organizaciones, la prevención, investigación, descubrimiento y persecución de prácticas ilegales. **Entre otros propósitos que pretenden lograrse en el marco de dicha tendencia, pueden citarse: reforzar el potencial de autodetección en la corporación, mejorar su autorregulación, optimizar los flujos de información e, incluso, incentivar la delación en el -cada vez más complejo- escenario corporativo.** Las reformas del Código Penal operadas por LO 5/2010 y LO 1/2015 donde -a través de la *exención* de responsabilidad penal[8]- se premia a las personas jurídicas que han implementado eficazmente[9] programas de prevención e incorporado órganos proactivos de compliance dentro de su diseño institucional, constituyeron claras muestras de esta estrategia; otro ejemplo de norma encuadrable en dicha tendencia fue la Ley 11/2018[10], singularmente, en lo concerniente a la imposición de presentar informe de Estado de Información No Financiera (EINF).

Esta tendencia de política criminal específicamente dirigida a combatir prácticas corruptas, fraudes y otros actos delictivos en contextos organizados no solo está focalizada sobre agentes y entidades del sector privado, sino que también tiene por objeto impregnar los procesos y organigramas del sector público. Por ello, el *Anteproyecto de Ley de Protección al Informante* impone obligaciones que afectan tanto a entes del sector privado como del público. En esta última esfera, podría considerarse que 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* (Mo de Hacienda y Función Pública) fue una de las disposiciones más recientes y remarcables, pues vino a exigir la implantación de un «plan de medidas antifraude» a aquellas entidades del Sector Público y cualesquiera otros agentes implicados en la ejecución como perceptores de los fondos europeos. «Plan de medidas antifraude»[11] que, en la práctica, constituye cuasi *compliance program* enfocado en el análisis, prevención, detección y respuesta eficaz frente a fraudes, corrupción y situaciones de conflicto de interés. Esto es, la citada Orden supuso la inserción del Compliance como instrumento autorregulatorio tendente a combatir irregularidades dentro del sector público.

Por tanto, podemos aseverar que, aunque el presente examen del *Anteproyecto de Ley de Protección al Informante* se centra en su virtualidad dentro del escenario empresarial, se trata de un texto que se ubica dentro de un planteamiento global de política criminal predominante y en expansión, que repercute

8. Respecto a los títulos de imputación o hechos de conexión para la atribución de responsabilidad penal de las personas jurídicas, *vid. Report. 3* Incertidumbres en el Compliance Penal: fragilidades con implicaciones reales para la empresa. «Beneficio corporativo indirecto», «incumplimiento grave de los deberes de supervisión», «nulidad de prueba en investigaciones internas y confidencialidad». Sobre la virtualidad de dichos programas en el ámbito del proceso penal, *vid. Report* 5. Tres Autos -cruciales- sobre compliance de la Audiencia Nacional: un análisis de los puntos clave de tres resoluciones judiciales dictadas en distintas investigaciones penales de relevancia que ilustran la especial trascendencia de los «sistemas de compliance».

9. En relación con la noción de eficacia de los programa de prevención de delitos, *vid. Report 2.* Refuerzo de la eficacia del Compliance: «*Behavioral Compliance*» y «*Nudges*». Recurso disponible en: https://www.grantthornton.es/contentassets/cf1d1a1829494b19b1ad4d934b073edc/report-2-compliance-advisory-lab.pdf

10. *Ley 11/2018, de 28 de diciembre, por la que se modifica el Código de Comercio, el texto refundido de la Ley de Sociedades de Capital aprobado por el Real Decreto Legislativo 1/2010, de 2 de julio, y la Ley 22/2015, de 20 de julio, de Auditoría de Cuentas, en materia de información no financiera y diversidad.* Disponible en: https://www.boe.es/buscar/doc.php?id=BOE-A-2018-17989. Como norma precedente, puede citarse la Ley 18/2017.

11. Sobre el contenido «plan de medidas antifraude», debe reseñarse el artículo 6 de la supracitada Orden:

Art. 6. Refuerzo de mecanismos para la prevención, detección y corrección del fraude, la corrupción y los conflictos de intereses: *«1.Con la finalidad de dar cumplimiento a las obligaciones que el artículo 22 del Reglamento (UE) 241/2021 del Parlamento Europeo y del Consejo, de 12 de febrero de 2021, impone a España en relación con la protección de los intereses financieros de la Unión como beneficiario de los fondos del MRR, toda entidad, decisora o ejecutora, que participe en la ejecución de las medidas del PRTR* ***deberá disponer de un «Plan de medidas antifraude» que le permita garantizar y declarar que, en su respectivo ámbito de actuación, 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.» […]***

En el **apartado 5 del precepto se concretan las exigencias mínimas** que ha de satisfacer el «plan de medidas antifraude», mientras que en el **apartado 6 se determina el modo de proceder de la entidad cuando detecte o tenga sospecha fundada de un posible fraude».** Recurso disponible en: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2021-15860

tanto sobre la actividad de las Administraciones públicas como del sector privado.

Pues bien, como se ha afirmado, **este texto tiene como propósito directo e inmediato el establecimiento de cauces y mecanismos de salvaguarda a aquellas personas físicas que alerten respecto a:**

1. **Infracciones de derecho comunitario.**
2. Conductas (activas u omisivas) **delictivas o de posible trascendencia penal.**
3. Las que puedan constituir una **infracción administrativa grave o muy grave.**
4. Comportamientos que pudieran constituir una **vulneración de cualquier disposición del ordenamiento jurídico siempre que perjudiquen o menoscaben el «interés general»** y no cuenten con regulación específica.

Como el lector puede extraer, se trata un *ámbito material* que desborda lo precisado en la Directiva «whistleblowing» (infracciones de derecho comunitario). Sin duda, extender el área de cobertura de los sistemas y mecanismos de protección al informante constituye una ventaja para el descubrimiento y persecución de incumplimientos; ahora bien, mientras que **los tres primeros supuestos fijados en el Anteproyecto permiten dibujar un horizonte algo más nítido sobre el *ámbito material* de la norma, el cuarto destaca por su extraordinaria amplitud y carácter difuso[12]:**

En primer lugar, porque si se habla de **transgresión de una *«disposición del ordenamiento jurídico»***, irremediablemente, ha de incardinarse en una regulación concreta (donde se enmarca el incumplimiento). En caso contrario, no existiría vulneración. Asimismo, si interpretamos la fórmula *«y no cuenten con una regulación específica»* de modo que se excluyan aquellas disposiciones que sí están dotadas de normas singulares de *protección al informante* (casi inexistentes), la amplitud e indeterminación quedan igualmente patentes.

En segundo término, porque el requisito de afectación o **menoscabo directo del *«interés general»* es, a todas luces, profundamente interpretable.** De hecho, podría llegar a entenderse que, cualquier actuación incívica que transgreda una norma o disposición prevista en el ordenamiento jurídico del que nos hemos dotado para garantizar la convivencia dentro de un Estado de derecho, afecta al interés general. Por ello, en el apartado II de la *Exposición de Motivos del Anteproyecto*, se apunta que están excluidas las normas de Derecho privado que abordan la *relación entre particulares*[13]. A su vez, el precepto incluye una cláusula que asevera cuando, en todo caso, se considera afectado el interés general: cuando la acción u omisión implique *«quebranto económico para la Hacienda Pública»*.

Sin embargo, en el articulado del Anteproyecto se dice, literalmente, que se incardinan dentro de su ámbito aquellas conductas que puedan ser constitutivas de «infracción **penal** o **administrativa grave o muy grave o cualquier vulneración del resto del ordenamiento jurídico…»**; es decir, engloba incumplimientos de normas que, no suponiendo infracciones de derecho administrativo, impactan -de algún modo- sobre el interés general. Y, resulta conocido que, el incumplimiento de preceptos situados fuera del perímetro de una infracción de naturaleza jurídico-pública, sí pueden llegar a desplegar efectos en el ámbito tributario, administrativo, etc. Igualmente, podrían traerse a colación noticias recientes sobre conductas claramente impropias que, no teniendo por qué constituir infracciones penales o administrativas, sí vulneran disposiciones

12. Literalmente, en la letra b) del apartado 2 del Artículo 1, se dice: *«Acciones u omisiones que puedan ser constitutivas de infracción penal o administrativa grave o muy grave o cualquier vulneración del resto del ordenamiento jurídico siempre que, en cualquiera de los casos, afecten o menoscaben directamente el interés general, y no cuenten con una regulación específica. En todo caso, se entenderá afectado el interés general cuando la acción u omisión de que se trate implique quebranto económico para la Hacienda Pública.»*

13. Se dice, textualmente, lo siguiente: *«Hay muchas infracciones tipificadas en el ordenamiento jurídico que responden a mecanismos de reacción frente a incumplimientos de normas de Derecho privado que regulan relaciones entre particulares y que, en consecuencia, no afectan al adecuado funcionamiento de las instituciones públicas y privadas que es, en definitiva, lo que se trata de preservar mediante la protección dispensada por esta ley. Interesa en este momento insistir en la protección del interés general sobre el que asientan y fortalecen los lazos de convivencia de una sociedad democrática. Por tanto, aquellos delitos e infracciones administrativas cuya tipificación se ha perfilado para reaccionar frente al daño al interés general son los que interesa perseguir y para ello la colaboración ciudadana es relevante.»*

Esta imprecisa frontera nos muestra **la primera problemática a la hora de armonizar la implementación de las obligaciones de esta futura norma con las previsiones que, respecto a los programas de prevención de delitos (o, en su caso, «sistemas de compliance»), contempla el propio Código Penal.** Recordemos que, en virtud de lo dispuesto en el requisito 4o del apartado 5 del 31 bis C.P., el «canal de denuncias» de este instrumento autorregulatorio engloba «riesgos e incumplimientos» y, si realizamos una interpretación sistemática del mismo tendiendo en consideración al quinto requisito, el incumplimiento de algún procedimiento o medida que contemple el propio programa de compliance es totalmente susceptible de ser denunciado vía canal de denuncias. ¿Refundimos el sistema interno con el canal de denuncias y dotamos de distintas garantías y cobertura al informante según se avise de un incumplimiento del programa de prevención o de otro incumplimiento que, no siendo delito o infracción administrativa, «pueda» «afectar» al «interés general»? ¿Otorgamos el mismo blindaje y cobertura al delator de una información o de otra? Sabemos, o nos podemos imaginar, que pueden darse este tipo de disyuntivas. Obviamente, un hecho delictivo implica la infracción del «sistema de compliance» -o debería serlo si se ha configurado adecuadamente-, **pero no todo incumplimiento del «sistema de compliance» constituye un delito (puede ser una mera trasgresión de la autorregulación);** por ejemplo, el incumplimiento de ciertos procedimientos o la elusión de controles que, si bien se aplican con el objeto de prevenir un delito, no conlleva la comisión de delito alguno (pues se trata de preceptos autorregulatorios tendentes a prevenir o reducir las posibilidades de comisión del delito, pero su incumplimiento no supone per se un delito).

En todo caso, las dudas emergerán cuando un **sujeto alerte o informe sobre un incumplimiento de alguna disposición que pueda tener «ciertas» implicaciones en el ámbito jurídico-público,** sin que exista un menoscabo evidente o directo al erario o sin que constituya una infracción penal u administrativa. ¿Afecta el concreto incumplimiento denunciado al interés general? ¿Sí? ¿No? Desde esta última postura, no se otorgaría la cobertura que dota la ley al denunciante o informante, por lo que el asunto no resulta trivial.

Y es que, a falta de mayor concreción, las razones que se viertan en uno u otro sentido podrán constituir sólidos argumentos -o vagos pretextos- para que, en la persona jurídica u organización, se considere que el aviso o información es -o no es- susceptible de activar el mecanismo de protección sobre el informante.

En consecuencia, el temor -fundado- por parte del informante a que el incumplimiento del que alerta sea considerado como un asunto excluido del ámbito de la norma, junto con una formación inadecuada en la corporación puede desembocar en:

a **que el denunciante no se atreva a informar,** si no tiene claro que el asunto del que alerta tiene trascendencia penal o es una infracción administrativa, por temor a quedar desprotegido o

b **que se aventure a argumentar que se trata de un delito o infracción administrativa** a pesar de no tener certeza de dicha naturaleza, con las implicaciones que ello genera.

Por tanto, considero que, si durante la tramitación del proyecto de ley, la cuestión no se clarifica -dentro del propio articulado-, esta problemática puede emerger con cierta regularidad y constituir una parte relevante de las incidencias.

En lo concerniente a los sujetos que protege la norma, procede subrayar que incluye tanto a personas físicas como jurídicas. En particular, el ámbito de personal de aplicación de esta norma comprende a: *trabajadores por cuenta ajena y autónomos; empleados del sector público; accionistas, miembros de consejos de administración y órganos de supervisión; personas que trabajen para contratistas, subcontratistas y proveedores, becarios, trabajadores en formación, así como aquellos que haya finalizado la relación laboral, y aquellos que todavía no la hayan iniciado (infracciones en procesos de selección o negociación contractual).* También engloba dentro de los beneficiarios de las medidas de protección (que se expondrán más adelante) a los representantes legales de los trabajadores, compañeros y sujetos que asistan al informante[14] durante el propio proceso, compañeros, familiares y personas jurídicas para las que trabaje el informante, mantenga vinculación laboral o participación significativa (si la persona tiene capacidad para influir en la persona jurídica participada).

Como puede deducirse, el ámbito personal resulta amplísimo, aspecto que, en principio, parece positivo. Con todo, podrá observarse que hay conceptos cuya delimitación puede resultar compleja. Una vez sea aprobada la norma, los juzgados y tribunales coadyuvarán a perfilar ese ámbito; asimismo, las *directrices y recomendaciones*[15] que dictará la futura *Autoridad Independiente de Protección al Denunciante* (cuya creación contempla el Anteproyecto y que se tratará más adelante) tendrán un papel relevante a la hora de solventar cuestiones de carácter interpretativo y operativo.

14. Con la finalidad de eludir connotaciones negativas, la ley denomina «informantes» a quienes tradicionalmente hemos denominado «denunciantes», «delatores» o, más coloquialmente «chivatos».

15. Sin perjuicio de ulterior tratamiento, puede adelantarse que se regulan en el artículo 43.7 (aunque no aparecen los apartados 5,6 y parece haber un error al señalar el numeral), mientras que en artículo 51 se hace alusión a las «Circulares y recomendaciones» como formas de materializar la potestad regulatoria de la *Autoridad Independiente de Protección al Informante*. Por otra parte, aunque no se trate de una ley -y carezca de virtualidad directa en el proceso- el estándar ISO 37002 sobre sistemas de gestión de la denuncia de irregularidades podría jugar un papel a la hora de interpretar ciertos conceptos. Sobre los procesos de estandarización y normalización, *vid.* página 8 del *Report 3. Incertidumbres en el Compliance Penal: fragilidades con implicaciones reales para la empresa. «Beneficio corporativo indirecto», «incumplimiento grave de los deberes de supervisión», «nulidad de prueba en investigaciones internas y confidencialidad».*

2. «Sistemas internos de información» (y la figura del «responsable»)

El establecimiento del «sistema interno de información» conforma, junto con la aplicación de *medidas de protección al informante* que haga uso del mismo, uno de los dos principales grupos de exigencias que esta ley contempla para empresarios y personas jurídicas. Este sistema interno ha de ser implantado por el órgano de administración o de gobierno y debe permitir a los sujetos ya señalados (ámbito personal) transmitir los tipos de avisos o informaciones a los que se ha hecho referencia en el apartado anterior (ámbito material).

El sistema debe configurarse de modo que **garantice la confidencialidad** del informante y permitir **comunicaciones escritas o verbales.** Ahora bien, en este punto relativo a qué modo de comunicación debe posibilitar el sistema de información surge una duda: cuando el apartado c) del artículo 5 del Anteproyecto señala que el sistema de información interna debe «*permitir la presentación de comunicaciones por escrito o verbalmente, o de ambos modos*» parece deducirse que se tratan de alternativas (disyuntiva) por el recurso a la conjunción «o». Por tanto, cabría entender que puede optarse (1) bien por un sistema que permita comunicaciones verbales, (2) bien por un sistema que permita comunicaciones escritas o (3) bien por otro sistema que permita ambos tipos de comunicaciones. Por su parte, el artículo 7 redunda en ese particular. Si se entiende que el sistema ha de permitir comunicaciones de ambos tipos, entiendo que lo adecuado hubiese sido recurrir a la conjunción copulativa «y». De ese modo, se evitan las lógicas dudas a la hora de elegir cómo configurar el sistema, pues no quedan demasiado lejos las cuestiones interpretativas arrojadas sobre el 31 bis del Código Penal, letra a) «*en nombre "o" por cuenta*» y letra b) «*en el ejercicio de actividades sociales "y" por cuenta*»[16].

Las organizaciones deben disponer de una **política que recoja los principios generales sobre sistemas internos y de defensa del informante,** tal política ha de ser adecuadamente difundida. Asimismo, el sistema interno de información debe disponer de un ***procedimiento de gestión de las informaciones recibidas*** y garantizarse **que dichos avisos o informaciones son conocidos, en primer lugar, por el propio empleador** (y, a su vez, que las informaciones son tratadas de manera efectiva dentro del ente).

El texto prevé la posibilidad de que la «gestión» del sistema pueda llevarse a cabo por un tercero -externo- en el confuso artículo 6[17]. Por gestión debe entenderse la *recepción* de informaciones. Igualmente, no debe confundirse «gestión» del sistema por un externo con la noción «canal externo» de comunicaciones (que, como veremos, es el cauce por el cual el informante puede informar del incumplimiento a la *Autoridad Independiente de Protección del Informante*).

16. *vid.* AGUILERA GORDILLO, R.; *Manual de Compliance Penal en España (2a Edición)*, Ed. Aranzadi, Pamplona, 2022. En particular, epígrafe 1.3. *La vinculación entre la conducta de la persona física y la persona jurídica como elemento específico de cada uno de los dos «hechos de conexión»: A. La actuación en nombre o por cuenta de la persona jurídica. B. La actuación en el ejercicio de actividades sociales y por cuenta de la persona jurídica*, pp. 351-357; o DEL ROSAL BLASCO, B.; «Responsabilidad penal de las personas jurídicas: títulos de imputación y requisitos para la exención», en AAVV/MORILLAS CUEVA (Dir.); *Estudios sobre el Código Penal reformado (Leyes Orgánicas 1/2015 y 2/2015)*, Ed. Dykinson, Madrid, 2015, pp. 84-85. También de interés GÓMEZ TOMILLO, M.; «Imputación objetiva y culpabilidad en el Derecho Penal de las personas jurídicas. Especial referencia al sistema español», en *Revista Jurídica de Castilla y León*, núm. 25, septiembre 2001, pp. 50-54; o FEIJOO SÁNCHEZ B.J.; «Cap. IV Los requisitos del Art. 31 bis 1», en BAJO HERNÁNDEZ, M./ FEIJOO SÁNCHEZ, B.J./ GÓMEZ-JARA DÍEZ, C.; *Tratado de responsabilidad penal de las personas jurídicas* (2.a Ed.), Ed. Aranzadi, Pamplona, 2016, pp. 75-88.

17. Un punto -crítico- reseñable es la equívoca afirmación que contiene sobre su responsabilidad. Así, en el apartado 3. del Artículo 6 se dice lo siguiente: «*3. La gestión del sistema interno de información por un tercero no podrá suponer un menoscabo de las garantías y requisitos que para dicho sistema establece la presente ley ni una atribución de la responsabilidad sobre el mismo en persona distinta del Responsable del Sistema*». ¿Quiere decirse que el responsable del sistema (que debe ser interno de la persona jurídica) va a ser siempre el sujeto que detente toda responsabilidad en relación al sistema o, en cambio, lo que se quiere decir es que el tercero gestor del canal no tendrá mayor ni menores responsabilidades en el marco de su actuación que la del responsable del sistema? De entender procedente la primera interpretación, debe cerciorarse la adecuada recepción de informaciones y avisos por parte del responsable del sistema. Esta interpretación resulta, asimismo, compatible con la 4a exigencia que el Código Penal prevé respecto a los programas de prevención de delitos en el apartado 5 del 31 bis C.P. (4.o *Impondrán la obligación de informar de posibles riesgos e incumplimientos al organismo encargado de vigilar el funcionamiento y observancia del modelo de prevención).* En consecuencia, si -como el Anteproyecto posibilita en el apartado 6 del artículo 9- el compliance officer es, a su vez, responsable del sistema, se produce una adecuada compatibilización en el cumplimiento de exigencias. Por otra parte, en el ámbito de protección de datos, este sujeto externo será considerado encargado del tratamiento.

Además, este precepto contempla que, en la *gestión del sistema por un tercero externo*, deberán aplicarse garantías adecuadas de respeto de la **independencia, confidencialidad, protección de datos y secreto.** Sobre la confidencialidad, sin perjuicio de lo que unas páginas más adelante se va a exponer sobre la figura del «responsable del sistema» y el «derecho a la no autoincriminación» de la persona jurídica, cabe avanzar que **se echa en falta una mayor concreción sobre el alcance y solidez de tal prerrogativa en esta futura ley que permita pacificar las diversas interpretaciones y jurisprudencia sobre requerimientos y aportación de documental que, según el caso, podrían incriminar al ente;** a *fortiori* cuando el apartado 1 del **artículo 26 del Anteproyecto recoge una estipulación que parece colisionar frontalmente con el nemo tenetur de la persona jurídica**[18]**:**

> ***«Artículo 26. Registro de comunicaciones.***
>
> *1. Todos los sujetos obligados, de acuerdo con lo dispuesto en esta ley, a disponer de un canal interno de informaciones, con independencia de que formen parte del sector público o del sector privado, deberán contar con* ***un libro-registro de las comunicaciones recibidas y de las investigaciones internas*** *a que hayan dado lugar, garantizando, en todo caso, los requisitos de confidencialidad previstos en esta ley19. Este registro no será público y* ***únicamente a petición razonada de la Autoridad judicial competente, mediante auto, y en el marco de un procedimiento judicial y bajo la tutela de aquélla, podrá accederse total o parcialmente al contenido del referido registro.»***

Por otro lado, el *Anteproyecto de Ley de Protección al Informante* distingue conceptualmente entre «sistema de información interna» y «canales internos de información». Mientras que **el sistema integra y vertebra todos los elementos implicados en la configuración y ejecución** (políticas, procedimiento de tramitación, garantías, figura del responsable, etc.), **el «canal» es el cauce o vía singular por donde se traslada la concreta información o aviso,** es decir, constituye uno de los elementos del sistema. En este sentido, la norma apunta que todos los canales internos de información de que disponga una entidad para posibilitar la comunicación de infracciones han de estar insertos dentro del «sistema interno de información». **En relación con estos canales de denuncias internos, se advierte que deben permitir la remisión de denuncias anónimas.** Asimismo, ha de posibilitarse la remisión del aviso o información de modo *presencial*[20].

El ***procedimiento de gestión* de los avisos o comunicaciones constituye otra obligación** que han de cumplir las personas físicas y jurídicas que cuenten con más de 49 trabajadores.

18. Aunque volveremos a esta cuestión, la tramitación del texto como proyecto de ley podría ser una oportunidad excelente para tratar la amplitud del blindaje del sistema de información interna y las futuras implicaciones de lo que ahora contempla el artículo 26. Asimismo, por la entidad de la materia que afecta el borrador, el Anteproyecto de Ley Orgánica de Derecho a la Defensa (cuya previsible tramitación se está demorando) puede constituir otra oportunidad para perfilar tan relevante cuestión, garantizando plenamente -y sin margen a equívocos- a las personas jurídicas lo dispuesto en el artículo 24 de la Constitución.

19. Negrita y subrayado añadidos.

20. El Anteproyecto 10 el apartado 2 del artículo 7. A su vez, dicho apartado señala que las *«comunicaciones verbales»* deben documentarse de alguno de estas formas: *«a) mediante una grabación de la conversación en un formato seguro, duradero y accesible, o b) a través de una transcripción completa y exacta de la conversación realizada por el personal responsable de tratarla.»*

Este procedimiento debe ser aprobado por el responsable del sistema (figura que se analizará a continuación), que detenta la responsabilidad de su diligente tramitación. El Anteproyecto fija los siguientes **principios y contenidos mínimos que deben contener el procedimiento de gestión de comunicaciones:**

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

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

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

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

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

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

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

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

i **Respeto de las disposiciones sobre protección de datos personales…**

El texto del Anteproyecto incluye una serie de especificidades de los sistemas de información interna que resultan diferentes en función de si nos encontramos con agentes o entes obligados del sector privado o del sector público[21] y, como se avanzaba, **dentro del sector privado, resultan obligadas a cumplir con lo dispuesto en la norma:**

- **LAS PERSONAS FÍSICAS O JURÍDICAS DEL SECTOR PRIVADO QUE TENGAN CONTRATADOS 50 O MÁS TRABAJADORES, ENGLOBANDO A LAS PERSONAS JURÍDICAS QUE SIN TENER DOMICILIO EN ESPAÑA DESARROLLEN ACTIVIDADES EN NUESTRO PAÍS (a través de agentes, sucursales o mediante la mera prestación de servicios sin establecimiento permanente). Cuando se trate de GRUPOS DE SOCIEDADES, el texto permite que se conforme un sistema interno de información y designe un responsable del mismo para todo el grupo o parte del mismo, pudiendo realizar las adaptaciones o adecuaciones necesarias.**
- **Los partidos políticos, los sindicatos, las patronales y las fundaciones creadas por unos y otros, siempre que reciban o gestionen fondos públicos.**

Sin perjuicio de lo anterior, **si el empresario o persona jurídica dispone de menos de 249 empleados, la norma posibilita que se puedan compartir con otros sujetos,** tanto el propio sistema interno de información como los recursos destinados a la gestión y tramitación de las comunicaciones (respetando las garantías previstas).

Como se indicaba, un aspecto sustantivo que, sobre estos sistemas, recoge el *Anteproyecto de Ley de Protección al Informante* es que debe designarse un «responsable del sistema interno de información». La figura del responsable del sistema sopone un punto especialmente sensible y, en muchos casos, determinará cambios en el diseño institucional de la persona jurídica. En primer lugar, el Anteproyecto afirma que la **identificación de este responsable** del sistema debe realizarla el órgano de administración o de gobierno de cada ente y que esta designación ha de trasladarla a la antes aludida *Autoridad Independiente de Protección al Informante* en un plazo de 10 días hábiles[22]. Por otra parte, el responsable puede ser una persona física o varias constituidas en órgano colegiado. **No obstante, con el evidente propósito de dotar la relevancia que merece esta función y de que, llegado el caso, se puedan esclarecer responsabilidades (incluidas las penales)** con mayor facilidad, el texto asevera, en los apartado 2 y 5 del artículo 9, lo siguiente:

> *«Artículo 9. Responsable del sistema interno de información.[..]*
>
> *2. Si se optase por que el Responsable del Sistema fuese un órgano colegiado, **éste deberá delegar en uno de sus miembros las facultades de gestión del sistema interno de información y de tramitación de expedientes de investigación.***
>
> *[…]*

21. Las particularidades de los sistemas de información interna para entes u agentes obligados del sector privado se contemplan en los artículos 10 a 12 y para los entes del sector público en los artículos 13 a 15. Dado que el presente análisis tiene como propósito el examen de las exigencias e implicaciones en el ámbito corporativo privado, no se incorpora el estudio de las exigencias y efectos de esta norma sobre el sector público, pues desbordaría el objeto del *report*.

22. Los ceses del responsable del sistema también deben ser notificados a esta autoridad, incorporando los argumentos que justifiquen tal decisión.

> 5. *En el caso del* ***sector privado, el Responsable del Sistema persona física o la persona en quien el órgano colegiado responsable haya delegado sus funciones, será un alto directivo de la entidad, que asumirá exclusivamente dichas funciones y que ejercerá su cargo con independencia del órgano de administración o de gobierno de la misma.*** *Cuando la naturaleza o la dimensión de las actividades de la entidad no justifiquen o permitan la existencia de un directivo Responsable del Sistema, será posible el desempeño ordinario de las funciones del puesto o cargo con las de Responsable del Sistema, tratando en todo caso de evitar posibles situaciones de conflicto de interés.»*[23]

Y es que, las autoridades son buenas conocedoras de las complejidades asociadas a la atribución de responsabilidades cuando intervienen órganos colegiados que detentan determinadas funciones dentro de escenarios corporativos, muy particularmente en el terreno jurídico-penal[24] o de estrategias consistentes en tratar de derivar funciones a profesionales de la abogacía externos con la idea de que, llegado el caso, se alegue la aplicación del «legal privilege» del abogado «defensor»[25]. Por ello, en el **Anteproyecto se asigna -con claridad meridiana- las concretas tareas de gestión del sistema y tramitación del expediente de investigación a una persona física, que será directa e inmediatamente responsable y que, además, ha de ser directivo de la propia persona jurídica.**

Además, sobre este sujeto el texto del Anteproyecto indica que, en las entidades donde ya existiera un responsable de la función de cumplimiento normativo, aquel podrá ser la persona designada como responsable del sistema interno de información (si cumple los requisitos establecidos en esta ley). La norma, por tanto, pretende facilitar el encaje con las estructuras orgánicas de compliance que ya existen en aquellas personas jurídicas con programas o «sistemas de compliance» implementados. No obstante, aunque se trata de una previsión acertada, la realidad empresarial se muestra más compleja y, hoy día, más que un único órgano, existen diversos órganos altamente especializados que se ocupan de distintas tareas ligadas al compliance. Más propio, quizás, hubiese sido apuntar a la compatibilidad con el sujeto responsable del «canal de denuncias» (aunque, nuevamente, emerge la disyuntiva sobre el ámbito material señalada al comienzo de este *report* acerca de cómo dar la respuesta más adecuada a aquellos incumplimientos que quedan fuera del ámbito de esta norma). En todo caso, la nítida designación de una persona física con facultades de gestión del sistema interno de información y en materia de tramitación de expedientes de investigación, **puede situar a este «responsable del sistema interno de información» en un eventual escenario de responsabilidad penal si omite o no actúa de manera procedente ante la recepción de una información que alerte sobre un posible delito.**

23. Negrita y subrayado añadidos.

24. *Vid.* ESTRADA I CUADRAS, A.; «Intervención delictiva a través de las decisiones de órganos colegiados de la empresa. Responsabilidad penal por comisión activa», en *La Ley Compliance Penal* no4, marzo, 2021. Igualmente, resulta de utilidad orientativa (pues este Anteproyecto confiere la facultad ejecutiva o, si se quiere, seudoejecutiva de tramitar las denuncias al responsable del sistema) MARTÍNEZ DE BUJÁN PÉREZ, C.; «*Autoría y participación de los órganos de administración en el ámbito de las estructuras empresariales*», en *La Ley Compliance Penal* no3, diciembre, 2020.

25. Sobre el legal privilege, vid. epígrafe 3. *Nulidad de prueba en investigaciones internas y confidencialidad* del Report. 3 Incertidumbres en el Compliance Penal: fragilidades con implicaciones reales para la empresa: «Beneficio corporativo indirecto», «incumplimiento grave de los deberes de supervisión», «nulidad de prueba en investigaciones internas y confidencialidad». Por su parte, el artículo 39 del Estatuto de la Abogacía Española (aprobado por Real Decreto 135/2021, de 2 de marzo), parece extender el *legal privilege* dentro de la empresa (contraviniendo la tendencia jurisprudencial a nivel europeo), pero únicamente a aquellos juristas de la organización que desempeñen -realmente- el rol de abogado, excluyendo esa confidencialidad frente a las autoridades cuando desempeña otro tipo funciones que sí pueden o podrían desarrollar otros individuos de la empresa. Para profundizar, *vid.* GOENA VIVES, B.; «Responsabilidad penal de las personas jurídicas y nemo tenetur: análisis desde el fundamento material de la sanción corporativa», en *Revista Electrónica de Ciencia Penal y Criminología*, núm. 23-22, 2021, pp 1-52.

26. Ampliamente sobre la responsabilidad penal de los órganos corporativos con funciones ligadas al canal de denuncias, *vid.* AGUILERA GORDILLO, R.; *Manual de Compliance Penal en España*, Ed. Aranzadi (2a Ed.), Pamplona, 2022.

Se trata de un escenario idéntico al del *compliance officer* que detenta la concreta función de decidir acerca del inicio/tramitación de un aviso o denuncia interna recibido vía canal de denuncias en el marco de ejecución del «sistema de compliance»; aspecto especialmente destacado por la propia Fiscalía General del Estado en su Circular 1/2016[27]:

> *«...la exposición personal al riesgo penal del oficial de cumplimiento no es superior a la de otros directivos de la persona jurídica. Comparativamente,* ***su mayor riesgo penal sólo puede tener su origen en que, por su posición y funciones, puede acceder más frecuentemente al conocimiento de la comisión de hechos delictivos, especialmente dada su responsabilidad en relación con la gestión del canal de denuncias*** *y siempre que la denuncia se refiera a hechos que se están cometiendo y que, por tanto, el oficial de cumplimiento pueda impedir con su actuación.»*

Por esta razón, resultaría absolutamente pertinente que el directivo designado para ocupar esta nueva posición dentro de la empresa tenga extensos conocimientos jurídico-penales y en materia de investigaciones internas o que, en su defecto, vaya a recibir un adecuado asesoramiento especializado que le permita desempeñar de manera adecuada -y con los menores sobresaltos posibles- las funciones conferidas.

27. Circular 1/2016 FGE (pp. 44-50).

3. «Canal externo de comunicaciones» y «disposiciones comunes» para canales internos y externos

El *Anteproyecto* **concreta un procedimiento[28] aplicable al singular cauce que posibilita que toda persona física pueda informar de incumplimientos a la nueva *Autoridad Independiente del Protección del Informante*** y que denomina «canal externo de comunicaciones». En este caso, nos encontramos, por tanto, con un canal que sí puede ser utilizado por cualquier individuo, sin matiz o restricción de ningún tipo. El procedimiento detalla el modo de *recepción de las comunicaciones* (donde se incide en la posibilidad del aviso anónimo y en la configuración de un registro que salvaguarde toda la información de manera segura), *trámite de admisión* (que aborda aspectos como el plazo para adoptar esta decisión o causas de inadmisión), *instrucción* (donde se señalan las garantías del investigado y deber de colaboración de otros sujetos), *terminación* (que concreta el contenido del informe con el que han de culminarse las actuaciones y las decisiones que pueden adoptarse) y los *derechos del informante*. Algunos de estos puntos contenidos en el procedimiento del canal externo pueden tener un valor orientativo a la hora de mejorar el procedimiento interno de investigación de avisos o informaciones en el seno de las empresas.

A este canal externo puede recurrirse, bien directamente o bien de tras haber acudido a un canal interno (si el sujeto estaba legitimado para ello). A su vez, el texto señala que la citada Autoridad Independiente será competente para tramitar las comunicaciones recibidas por el canal externo de los asuntos que afecten al sector público privado, cuando la infracción afecte o produzca sus efectos en más de una comunidad autónoma, y al sector público estatal, Casa del Rey y otros órganos constitucionales. Cuando los efectos se circunscriban al ámbito local o de una sola comunidad autónoma, el texto determina que esta Autoridad podría resultar competente en virtud de la firma de un Convenio cuando la respectiva comunidad autónoma no haya atribuido competencia para gestionar el canal externo a ningún órgano propio[29]. Así pues, puede extraerse que los **entes o agencias anticorrupción creados por las comunidades autónomas (o aquellos de futura creación) resultarían competentes** para tramitar avisos o comunicaciones recibidas que solo tengan efectos dentro de una comunidad autónoma, por lo que se haría uso de sus respectivos canales externos. **La Oficina Antifraude de Cataluña[30], la Agencia de Prevención y Lucha contra el Fraude y la Corrupción de la Comunitat Valenciana[31], la Oficina Andaluza contra el Fraude y la Corrupción en Andalucía y Protección de la Persona Denunciante[32] o la Oficina de Prevenció i Lluita contra la Corrupció a les Illes Balears[33]** son ejemplos de entes autonómicos con personalidad jurídica propia que detentan las potestades vinculadas a la materia dentro de sus respectivos ámbitos autonómicos (la descentralización en este campo parece resultar un fenómeno en expansión).

28. Artículos 17-21 del Anteproyecto.

29. El Anteproyecto de Ley de Protección al Informante recoge, en la letra b) del artículo 24:

«Artículo 24. Autoridades competentes.

1. La Autoridad Independiente de Protección del Informante regulada en el título VIII es la autoridad competente para la tramitación, a través del canal externo, de las comunicaciones que afecten a los siguientes sujetos:[…]

b) Las Administraciones de las comunidades autónomas, a las entidades que integran la Administración y el sector público institucional autonómico o local, cuando se atribuya la competencia a la Autoridad Independiente de Protección del Informante por virtud de un convenio o cuando la respectiva comunidad autónoma no haya atribuido competencia para gestionar el canal externo de informaciones a ningún órgano o autoridad propios. […]»

30. Creada por Ley 14/2008, de 5 de noviembre. Web: https://www.antifrau.cat/es/es

31. Constituida mediante Ley 11/2016, de 20 de noviembre. Web: https://www.antifraucv.es/

32. Creada por Ley 2/2021, de 18 de junio. Web (pend. desarrollo): https://www.juntadeandalucia.es/organismos/transparencia/informacion-institucional-organizativa/organizacion-institucional/paginas/oficina-contra-fraude.html

33. Constituida por Ley 16/2016, de 9 de diciembre, de creación de la Oficina de Prevención y Lucha Contra la Corrupción en las Illes Balears. Web: https://www.oaib.es/

En relación con las «disposiciones comunes aplicables a canales internos o externos», el **precepto más trascendental que contiene este *Anteproyecto de Ley de Protección al Informante* es el referido a la llevanza del *libro-registro de comunicaciones*[34] recibidas e investigaciones internas desarrolladas (que será confidencial),** con la controvertida afirmación de que «*a petición razonada de la Autoridad judicial competente, mediante auto, y en el marco de un procedimiento judicial y bajo la tutela de aquélla, podrá accederse total o parcialmente al contenido…*».

Indudablemente, se trata de un precepto que, hasta el momento, no ha llamado demasiado la atención de los profesionales del Compliance (quizás, porque nos encontramos en fase embrionaria de la norma). Pero lo que puede parecer una ventaja (la llevanza del libro-registro), **puede comprometer el «derecho a la no autoincriminación» de la persona jurídica -sometida investigación- cuando en este mismo precepto se contempla que un juzgado puede acceder a su contenido de manera total o parcial.**

Parece necesario que, durante la tramitación de la norma, se revise este artículo 26 y se recapacite sobre sus **implicaciones para el ejercicio -efectivo- del derecho a la defensa de la persona jurídica que está siendo investigada.** Sobre ello, pueden lanzarse las dos siguientes reflexiones:

1 **No se concreta qué nivel de información debe almacenarse en el *libro-registro*.** De la lectura del artículo, no queda claro si debe contener algunos datos relativos a fecha, sujetos implicados, etc. de las comunicaciones recibidas y las investigaciones desarrolladas o si, en cambio, debe almacenarse toda la documental recibida y generada durante el desarrollo de los procesos de investigación. Y es que, como registro, se suele entender al listado con datos generales -o asientos- recogidos a modo de índice, que permiten discriminar distintos hechos o aspectos[35]. Resulta evidente que el grado de información almacenada en este registro repercutirá, directamente, en la cantidad de información que, llegado el caso, tendría que facilitarse a la autoridad judicial.

2 **Como se expuso en el epígrafe 3 del report 5[36], los requerimientos de documentos ligados al canal de denuncias y desarrollo de las investigaciones internas (en la ejecución de los «sistemas de compliance») afectan al derecho a la no autoincriminación de la persona jurídica.** Es cierto que el supuesto es distinto, pero nos permite advertir como una obligación de este tipo puede transgredir directamente la no autoincriminación del sujeto (y esta afectación, como mínimo, requeriría ponderación / previsión en ley orgánica). En el aludido report se analizaba un **requerimiento del juzgado de instrucción que pedía la persona jurídica la totalidad de las denuncias internas y los expedientes generados[37].** Ante el recurso de la defensa, el tribunal de apelación (sección 4a de la Sala de lo Penal de la Audiencia Nacional) revocó tal requerimiento -haciendo alusión a la jurisprudencia del Tribunal Europeo de Derechos Humanos y del Tribunal Constitucional[38]- y expuso que, en el curso del proceso penal dirigido contra la persona jurídica, no puede requerirse la aportación de documentos

34. También se establece el período máximo de conservación de los datos personales (10 años), bajo la máxima de que, en todo caso deberán respetarse las exigencias relativas a protección de datos.

35. De las distintas acepciones de la RAE, extraemos por su vinculación con el objeto del estudio la 8, 9,10, 11,12 y 22: *9. m. Asiento que queda de lo que se registra; 10. m. Cédula o albalá en que consta haberse registrado algo; 11. m. Libro, a manera de índice, donde se apuntan noticias o datos; 12. m. Índice o lista de personas o cosas que se consignan para un fin determinado; 22. m. Inform. Conjunto de datos relacionados entre sí, que constituyen una unidad de información en una base de datos.*

36. report 5. *Tres Autos -cruciales- sobre compliance de la Audiencia Nacional: un análisis de los puntos clave de tres resoluciones judiciales dictadas en distintas investigaciones penales de relevancia que ilustran la especial trascendencia de los «sistemas de compliance».*

37. En la Providencia emitida por el juez instructor se requería a la persona jurídica investigada que aportara, entre otra, la siguiente documental: «*Las copias certificadas de los programas de cumplimiento normativo (compliance) de "Abengoa, S.A." vigentes durante los años 2013 a 2016, así como de la totalidad de las denuncias internas de "Abengoa, S.A." recibidas a través del "canal de denuncias" durante los años 2013 a 2016, junto con los expedientes de tramitación de las mismas que se puedan haber generado...*»

38. STTEDH de fecha 3 de mayo de 2001 / STTJUE de 25 de enero de 2007.

39. Precisó que ese «derecho a la no autoincriminación» pueda hacerse valer es necesario que se trate de una medida de la autoridad tendente a la obtención de un documento o fuente de prueba «*cuya existencia dependa de la voluntad del investigado*», citada la STEDH de 17 de diciembre 1996. 33. La resolución cita, además, las siguientes sentencias del Tribunal Constitucional: STC núm. 76/1990, de fecha 20 de abril y STC núm. 161/1997, de fecha 2 de octubre.

cuya existencia dependa de la exclusiva voluntad de la investigada[39].

En ese caso, al tratarse de documental dimanante de la ejecución del «sistema de compliance» (de adopción y ejecución totalmente voluntaria) no se plantean más incertidumbres. **La problemática de este nuevo precepto previsto en el Anteproyecto es que, de aprobarse, el *libro-registro* sí constituiría un tipo de documental cuya configuración y llevanza es obligatoria para empresarios y personas jurídicas con más de 49 empleados.**

¿Estaría obligada la persona jurídica investigada a aportar ese libro-registro?

Sobre tal interrogante, procede partir de las implicaciones del derecho a no autoincriminarse. El ***nemo tenetur se ipsum accusare* (nadie está obligado a autoincriminarse) comprende 3 derechos: derecho a guardar silencio, derecho a no declarar contra uno mismo y el derecho a no confesarse culpable.** Como se ha señalado, en España se está sosteniendo -vía jurisprudencial- que la persona jurídica es titular de los mismos derechos fundamentales y garantías que las físicas y que, en esta concreta esfera, también es beneficiaria del *nemu tenetur*[40]. Se trata de una postura, en principio, ampliamente respaldada por la doctrina. GÓMEZ TOMILLO, expone varios argumentos que apuntalan sólidamente de esta posición:

I Derecho a la no autoincriminarse del ente corporativo es el **correlato lógico de su condición de sujeto pasivo** de un proceso punitivo (penal o administrativo sancionador).

II Es coherente con el **fundamento mismo del derecho a no autoincriminarse,** pues se sustenta en

- a **derecho a la presunción de inocencia:** debe ser la acusación la que acredite los hechos constitutivos del ilícito.
- b **Derecho a la defensa:** la persona jurídica puede optar por una línea de defensa puramente pasiva (un simple no hacer para defenderse), totalmente legítima.

III No dotar a las personas jurídicas del derecho a no autoincriminarse **nos llevaría a una aporía;** ¿porque no respetamos ese derecho para el ente corporativo y sí otros (pj.: dcho. tutela judicial efectiva, dcho. inviolabilidad del domicilio, etc.) ¿Cuáles serían los criterios para excluir unos derechos a la persona jurídica y sí respetar otros?

Asimismo, este enfoque se ve reforzado a nivel procesal-penal, particularmente con las previsiones del artículo 409 bis y 786 bis de la Ley de Enjuiciamiento Criminal[41]. **Es más, se sostiene (con razón) que, para garantizar plenamente el derecho a «no autoincriminarse» de la persona jurídica, la distinción entre legitimidad de requerimientos de documentos cuya llevanza sea obligatoria e ilegitimidad de requerimientos cuya llevanza sea meramente voluntaria, no debe existir.** Por consiguiente, desde esta postura u opinión, la persona jurídica podría negarse a aportar cualquier tipo de documental -u otras evidencias- que pudieran servir para incriminarla, con independencia de si existe o no alguna norma que obligue a disponer de tal documento. **Precisamente, este sería el contexto en que nos situaríamos cuando se apruebe el contenido del Anteproyecto (una norma que impone la configuración y llevanza de un *libro-registro*).**

40. A nivel internacional la cuestión no resulta pacífica. El Tribunal Supremo de Estados Unidos ha aseverado en reiteradas ocasiones que las personas jurídicas no son titulares del derecho a no autoincriminarse. La Corte Interamericana fue consultada sobre si las personas jurídicas detentaban los derechos reconocidos para las personas jurídicas, dando una respuesta negativa, pero de forma ambigua y dejando las puertas abiertas a determinados extremos. El Tribunal Europeo de Derechos Humanos ni ha reconocido con meridiana claridad -ni ha negado- el derecho a no autoincriminarse.

41. *«Artículo 409 bis. **Cuando se haya procedido a la imputación de una persona jurídica, se tomará declaración al representante especialmente designado por ella, asistido de su Abogado.** La declaración irá dirigida a la averiguación de los hechos y a la participación en ellos de la entidad imputada y de las demás personas que hubieran también podido intervenir en su realización. A dicha declaración le será de aplicación lo dispuesto en los preceptos del presente capítulo en lo que no sea incompatible con su especial naturaleza, **incluidos los derechos a guardar silencio, a no declarar contra sí misma y a no confesarse culpable. […]»***

*Artículo 786 bis. 1. Cuando el acusado sea una persona jurídica, ésta podrá estar representada para un mejor ejercicio del derecho de defensa por una persona que especialmente designe, debiendo ocupar en la Sala el lugar reservado a los acusados. **Dicha persona podrá declarar en nombre de la persona jurídica si se hubiera propuesto y admitido esa prueba, sin perjuicio del derecho a guardar silencio, a no declarar contra sí mismo y a no confesarse culpable,** así como ejercer el derecho a la última palabra al finalizar el acto del juicio.*

No se podrá designar a estos efectos a quien haya de declarar en el juicio como testigo. […].

Y es que, si mantuviéramos que, únicamente, puede alegarse el derecho a la «no autoincriminación» cuando no exista previsión legal que obligue al ente a configurar y poseer una documentación concreta, estamos haciendo depender la aplicación -o no- de un derecho esencial del mero contenido de alguna norma de rango legal (cuando no reglamentario), **lo cual resulta extraordinariamente peligroso en términos de derechos fundamentales.**

Por otra parte, las circunstancias podrían volverse aún más complejas si la *Autoridad Independiente de Protección al Informante* (autoridad administrativa, no judicial) requiriera tal *libro-registro* a los efectos de comprobar el adecuado cumplimiento de las obligaciones previstas en la norma. Se trataría de algo similar a los requerimientos en el seno de procesos de inspección tributaria o en sectores regulados con posibles derivaciones penales[42]; sin embargo, a pesar de que la Autoridad puede realizar actuaciones para comprobar el cumplimiento de la norma, esa singular previsión no parece encontrar soporte explícito en el Anteproyecto (es más, de la lectura del artículo 26, debería deducirse lo contrario).

42. Para profundizar sobre esta cuestión, *vid.* GÓMEZ TOMILLO, M.; *Instrumentos jurídicos de tutela y ejecución de las potestades de inspección y supervisión administrativa de sociedades que operan en los mercados*, *Ed. Aranzadi*, *Pamplona*, *2019.*

4. «Revelación pública» y «protección de datos personales»

En principio, esta norma **no dota de cobertura a quienes transmitan públicamente, ya sea por redes, medios de comunicación cualquier otra vía, alguna de las irregularidades o incumplimientos** señalados al comienzo del *report*. En el preámbulo de la norma se justifica tal desprotección a quienes ponen a disposición del público información sobre incumplimientos por la tipología de *«garantías y protección que ofrece la opinión pública en su conjunto amparando a quien muestra una actitud cívica a la hora de advertir ante posibles delitos o infracciones graves o vulneraciones del ordenamiento jurídico que dañan el interés general, así como la protección de las fuentes que mantienen los periodistas»*. Sea o no sea, esta, una causa que legitime tal distinción, lo cierto es que la norma **sí contempla excepciones a esta desprotección.**

Para que un informante que haga pública la información sobre el incumplimiento pueda acogerse a la referida salvedad y, en consecuencia, **se beneficie de los mecanismos y garantías de protección al denunciante deben darse alguna de estas 2 circunstancias:**

- **que ya hubiera recurrido al canal interno o externo y no se hubieran adoptado medidas en el plazo conferido.**
- **que tenga motivos razonables para temer que existe un peligro inminente para el interés público (p. ej.: situación de emergencia, un riesgo de daños irreversibles, incluido un peligro para la integridad física de una persona, etc.) o que no recurriera al canal externo al preciar riesgo alto de represalias o pocas probabilidades de que se dé un tratamiento efectivo a la información.**

Como el lector podrá percibir, la segunda de las condiciones apela a nociones como riesgo alto[43], pocas probabilidades, etc. **Son conceptos que se prestan a diversas interpretaciones y que, además, varían en función de la percepción y contexto en que se sitúa cada sujeto[44].** No resulta aventurado pensar que se presentarán supuestos donde un informante, tras acudir a un medio de comunicación y denunciar públicamente un hipotético incumplimiento, reclame la cobertura que otorga esta norma bajo el argumento de que tenía temor fundado a recibir represalias o que entendía que las probabilidades de que atendieran su aviso eran escasas. Veremos como las resoluciones de la Autoridad y, llegado el caso, de los juzgados y tribunales interpretan estos conceptos[45].

Por otro lado, los artículos 29 a 34 del texto se ocupan del régimen y aplicación de las disposiciones en materia de protección de datos[46], dotando de licitud al tratamiento de datos personales para la aplicación de esta norma. Se recoge que **todos los agentes y entidades que resulten obligados a establecer un sistema de información interna deberán nombrar un «delgado de protección de datos»** que se ocupe de los tratamientos llevados a cabo en el sistema (exigencia que también se aplica a los terceros que gestionen dicho sistema).

43. Para profundizar en nociones ligadas a la percepción de la «probabilidad» en cuanto a riesgos y su vínculo con los «sesgos» o nociones como el dolo y la imprudencia (en particular, en marcos corporativos), *vid.* Report. 6 *Probabilidad del riesgo, dolo eventual e imprudencia consciente: examen de una difusa frontera entre la condena y la absolución de la persona jurídica.*

44. Otro ejemplo del recurso a estas nociones -con importantes efectos en el contexto corporativo- es lo dispuesto en el apartado 5 del artículo 38 del Anteproyecto.

45. La literalidad de esta segunda condición que ampara la cobertura prevista en la norma es la siguiente:

«…La persona que haga una revelación pública sólo podrá acogerse a protección en virtud de la presente ley si se cumple alguna de las condiciones siguientes: […]

b) Que tenga motivos razonables para pensar que:

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

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

46. Se recuerda el debido cumplimiento a lo contemplado en el Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos), en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos y garantía de los derechos digitales y en la *Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.*

Asimismo, **solo podrán acceder a los datos personales introducidos en el «sistema interno de información» del sujeto o corporación los siguientes profesionales (y siempre dentro del ejercicio de las funciones conferidas):**

- Responsable del sistema o que lo gestione directamente
- Responsable de recursos humanos, únicamente cuando proceda la aplicación de medidas disciplinarias contra un empleado
- Responsable de los servicios jurídicos, únicamente si proceden la adopción de medidas legales en función de lo relatado en el aviso
- Encargados de tratamiento designados
- Delegado de protección de datos

A pesar de ello, es lícito el tratamiento de estos datos por otros sujetos cuando sea necesario para tramitar procedimientos sancionadores o penales.

Tal y como contempla el actual artículo 24 de la *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales*, este Anteproyecto señala que **3 meses después de la recepción de la comunicación que se hubiera dado inicio a las actuaciones de investigación, deberá procederse a su supresión,** salvo que la finalidad de la conservación sea dejar evidencia del funcionamiento del sistema. Las comunicaciones a las que no se haya dado curso solamente podrán constar de forma anonimizada (sin que sea de aplicación la obligación de bloqueo prevista en el artículo 32[47] de la Ley Orgánica 3/2018, de 5 de diciembre).

Dado que el artículo 24 de la citada Ley Orgánica se vería modificado en virtud de la *disposición final cuarta* contenida en el *Anteproyecto de Ley de Protección al Informante* (que sería tramitada como proyecto de ley -ordinaria- ley y no como orgánica), muchos han denunciado que se trataría de un cauce impropio para alterar el contenido de un precepto[48] tan relevante de una ley orgánica.

Por su parte, el texto acentúa que **la identidad del informante debe mantenerse confidencial y solo podría comunicarse a la autoridad judicial, fiscalía o autoridad administrativa competente dentro del marco de una investigación penal, disciplinaria o sancionadora.**

47. Sobre en qué consiste el bloque de datos, el citado precepto expone: «*Artículo 32 Bloqueo de los datos.*

1. El responsable del tratamiento estará obligado a bloquear los datos cuando proceda a su rectificación o supresión.

2. El bloqueo de los datos consiste en la identificación y reserva de los mismos, adoptando medidas técnicas y organizativas, para impedir su tratamiento, incluyendo su visualización, excepto para la puesta a disposición de los datos a los jueces y tribunales, el Ministerio Fiscal o las Administraciones Públicas competentes, en particular de las autoridades de protección de datos, para la exigencia de posibles responsabilidades derivadas del tratamiento y solo por el plazo de prescripción de las mismas.

Transcurrido ese plazo deberá procederse a la destrucción de los datos.

3. Los datos bloqueados no podrán ser tratados para ninguna finalidad distinta de la señalada en el apartado anterior. […]».

48. Es cierto que, la disposición final en cuestión altera sustancialmente el contenido del artículo 24 Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales. El precepto quedaría, exclusivamente, con el siguiente contenido: «*Artículo 24. Tratamiento de datos para la protección de las personas que informen sobre infracciones normativas.*

Serán lícitos los tratamientos de datos personales necesarios para garantizar la protección de las personas que informen sobre infracciones normativas. Dichos tratamientos se regirán por lo dispuesto en el Reglamento (UE) 2016/679, en la presente ley orgánica y en la Ley …../…. de …., reguladora de la protección de las personas que informen sobre infracciones normativas y por la que se traspone 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.»

5. «Medidas de protección» de personas que comuniquen infracciones penales, comunitarias o administrativas que afecten al interés general y *programas de clemencia.*

El Título del *Anteproyecto de Ley de Protección al Informante* que aborda el despliegue de medidas de protección al informante[49] comienza señalando **las circunstancias que necesariamente han de concurrir para otorgar el derecho a la protección:** que el informante tenga ***«motivos razonables para pensar que la información referida es veraz*** *en el momento de la comunicación» (aunque no aporte pruebas concluyentes) y que esa comunicación* ***«se haya realizado conforme a los requerimientos previstos en esta ley».***

Para ambos supuesto, constituye presupuesto o ***«condicio sine qua non»*** **que se trate de una comunicación o información sobre una infracción situada dentro del *ámbito material*** (punto de importancia crítica abordado en el primer epígrafe del *report* y que, como expuse, existe cierto segmento[50] susceptible de generar numerosas controversias). Inmediatamente después **se establece la prohibición de aplicar cualquier tipo de represalia contra el informante.** El Anteproyecto concibe como represalia cualquier acto u omisión que suponga un trato desfavorable originado por dicha denuncia (excluyendo aquellas medidas justificadas y legítimas desligadas de aquella) y establece un criterio temporal asociativo ciertamente extenso; en particular, integra el siguiente **concepto de «represalia»[51]:**

«Se entiende por represalia cualesquiera actos u omisiones que estén prohibidos por la ley, o que, de forma directa o indirecta, supongan un trato desfavorable que sitúe a las personas que las sufren en desventaja particular con respecto a otra en el contexto laboral o profesional, sólo por su condición de informantes, o por haber realizado una revelación pública, y siempre que tales actos u omisiones se produzcan mientras dure el procedimiento de investigación o en los dos años siguientes a la finalización del mismo o de la fecha en que tuvo lugar la revelación pública. Se exceptúa el supuesto en que dicha acción u omisión pueda justificarse objetivamente en atención a una finalidad legítima y que los medios para alcanzar dicha finalidad sean necesarios y adecuados.»[52]

El Anteproyecto contempla una serie de **«medidas de apoyo para los informantes»[53]:** asesoramiento integral y gratuito sobre protección frente a represalias y derechos del informante; asistencia efectiva en su protección y, de manera extraordinaria (previa valoración de la Autoridad independiente de Protección del Informante), apoyo financiero y psicológico[54].

49. Título VII «Medidas de protección». Arts. 35 a 41.

50. El relativo a los incumplimientos de preceptos que, sin conllevar una infracción administrativa y penal o afectar directamente a la Hacienda pública, sí pueden generar efectos o implicaciones de trascendencia jurídico-pública. Asimismo, según el criterio que se acoja, el hecho de alertar sobre incumplimientos de procedimientos o mecanismo de control contemplados en los sistemas de compliance o modelos de prevención de delitos que no supongan un comportamiento delictivo, puede quedan dentro o fuera del mismo. Y es que, como resulta evidente, determinados incumplimientos del sistema de compliance podrían ser subsumibles en un injusto penal, pero otros muchos no.

51. Asimismo, en el apartado 3 del mismo precepto se contemplan algunos ejemplos de represalias:

«a) Suspensión del contrato de trabajo, despido o extinción de la relación laboral o estatutaria, incluyendo la terminación anticipada de un contrato de trabajo temporal una vez superado el período de prueba, o terminación anticipada o anulación de contratos de bienes o servicios, imposición de cualquier medida disciplinaria, degradación o denegación de ascensos y cualquier otra modificación sustancial de las condiciones de trabajo, salvo que estas medidas se llevaran a cabo dentro del ejercicio regular del poder de dirección al amparo de la legislación laboral o reguladora del estatuto del empleado público correspondiente, por circunstancias, hechos o infracciones acreditadas, y ajenas a la presentación de la comunicación. b) Daños, incluidos los de carácter reputacional, o pérdidas económicas, coacciones, intimidaciones, acoso u ostracismo. c) Evaluación o referencias negativas respecto al desempeño laboral o profesional. d) Inclusión en listas negras o difusión de información en un determinado ámbito sectorial, que dificulten o impidan el acceso al empleo o la contratación de obras o servicios. e) Anulación de una licencia o permiso.»

52. Subrayado añadido.

53. Sin prejuicio de los beneficios contemplados en la Ley de Asistencia Jurídica Gratuita para aquellos que puedan acogerse a esta.

54. Poco se dice acerca de cómo se articularán y financiarán. De momento, no disponemos de la memoria económica y la única previsión presupuestaria que contempla el Anteproyecto es la recogida en la disposición transitoria cuarta, que se circunscribe al soporte de los costes y gastos de la nueva *Autoridad Independiente de Protección del Informante*. Para comunidades autónomas con órganos competentes, el Anteproyecto señala que las medidas de apoyo al informante se prestarán por estos órganos (Art. 41).

En cuanto a las **«medidas de protección frente a represalias»,** el texto apunta a la completa **exención de responsabilidades a los informantes, pero determina con toda claridad que la citada medida no afecta a las posibles responsabilidad penales en que pudiera incurrir el informante.** A su vez, la norma refrenda la **inversión de la carga de la prueba en procesos laborales** ligados a perjuicios padecidos por el informante; por tanto, el sujeto que aplicó la medida gravosa para el informante debe acreditar que esta no constituyó una represalia por el aviso emitido, sino una medida legítima y debidamente justificada.

Asimismo, la norma **resulta asombrosamente lacónica en cuanto a la garantía de los derechos que asisten al investigado** o denunciado en la fase de tramitación del expediente, pues únicamente dice lo siguiente:

«Durante la tramitación del expediente las personas investigadas en la comunicación tendrán derecho a la presunción de inocencia, al derecho de defensa y de acceso al expediente en los términos regulados en esta ley, así como de la misma protección establecida en la misma para los informantes, preservándose su identidad y garantizándose la confidencialidad de los hechos y datos del procedimiento.»

Resulta, por tanto, palmaria la necesidad de contar con personal cualificado en el complejísimo terreno de las «investigaciones internas corporativas» y *Forensic* para tratar de asegurar el adecuado desarrollo de la investigación. Y es que, la práctica defectuosa de una actuación indagatoria dentro de dicha investigación puede acarrear la «inutilizabilidad» de la evidencia recabada e, incluso, arrastrar a todas aquellas obtenidas a partir de la originaria (en virtud de los efectos derivados de la «prueba ilícita» y la doctrina de los frutos del árbol envenenado)[55].

Para concluir este epígrafe, se considera oportuno subrayar la inclusión de los denominados **«programas de clemencia»** para incumplimientos de disposiciones o normas administrativas: **se establece la delación premiada a quienes informen o, mejor dicho, *confiesen* que han «participado» en un hecho que suponga infracción administrativa y el premio consiste en la exención del cumplimiento de la correspondiente sanción administrativa.**

Se trata de una notable ventaja a la hora de facilitar el descubrimiento de infracciones administrativas, pues incentiva sobremanera y de forma generalizada (engloba todo ámbito administrativo[56]) que se informe sobre incumplimientos «desde dentro». No obstante, la fórmula a la que recurre el texto para señalar a los posibles beneficiarios *(«persona que hubiera participado en la comisión de la infracción administrativa»)* arroja alguna duda sobre si quienes protagonizaron -o, *stricto sensu*, fueron autores principales- de la conducta infractora pueden ser beneficiarios del programa de clemencia. De la lectura del artículo, no puede deducirse con la necesaria claridad si se trata de una medida dirigida a partícipes (menos implicados en la infracción y que, por tanto, se les deja esta vía abierta) o a todo sujeto que interviene en la infracción (autores y partícipes).

Las condiciones que se exigen para poder beneficiarse de este mecanismo de delación premiada no ayudan a esclarecer esta duda puesto, como vamos a ver, la primera de estas cuatro exigencias requiere que el potencial beneficiario haya cesado en la «comisión de la infracción», lo que **puede entenderse como una fórmula que sí incluiría al autor o autores de la infracción:**

a. **Haber cesado en la comisión de la infracción en el momento de presentación de la comunicación o revelación e identificado, en su caso, al resto de las personas que hayan participado o favorecido aquella.**
b. **Haber cooperado plena, continua y diligentemente a lo largo de todo el procedimiento de investigación.**
c. **Haber facilitado información veraz y relevante, medios de prueba o datos significativos para la acreditación de los hechos investigados, sin que haya procedido a la destrucción de estos o a su ocultación, ni haya revelado a terceros, directa o indirectamente a terceros su contenido.**
d. **Haber procedido a la reparación del daño causado que le sea imputable.**

En cualquier caso, **cuando alguna o algunas de estas cuatro exigencias se cumplan de manera parcial por parte del informante, podría aplicarse la atenuación** de la sanción correspondiente, extremo que penderá del criterio de la autoridad sancionadora competente.

55. Para profundizar sobre prueba ilícita en las investigaciones internas y sobre los derechos y garantías del investigado, *vid.* apartado 1. *Investigaciones internas corporativas: «utilizabilidad» de las evidencias, delimitaciones de la jurisprudencia sobre ilicitud de prueba y autotutela de la empresa vs. empresa como «agente del Estado»* (Capítulo 5), *Manual de Compliance Penal en España.*

56. Hasta ahora, de manera predominante en el marco de la normativa de Defensa de la Competencia (Arts. 65 y 66 de la *Ley 15/2007 de Defensa de la Competencia)*; sobre ello, vid. apartado 4 del artículo 40.

6. «Autoridad Independiente de Protección del Informante» y «régimen sancionador»

El texto contempla la **creación y el régimen jurídico de la *Autoridad Independiente de Protección al Informante*** a la que se ha ido haciendo alusión a lo largo del presente informe. Este sujeto de Derecho Público estará compuesto por **Presidencia** (nombramiento por mayoría de la comisión competente del Congreso, previa propuesta del Mo de Justicia y con un mandato de 5 años) y por un **Consejo Asesor** (órgano que aconsejará a Presidencia y que estará compuesto por once miembros[57]). Esta Autoridad detentará la potestad sancionadora en el ámbito estatal y autonómico, cuando no le corresponda al órgano competente de la respectiva Comunidad Autónoma.

En lo que al sector privado se refiere, la Autoridad Independiente de Protección al Informante es competente sobre **aquellas infracciones cometidas cuando el incumplimiento informado afecte o produzca sus efectos en el ámbito territorial de más de una comunidad autónoma.** A la figura de Presidencia le corresponderá la facultad para imponer las sanciones que procedan.

La infracciones puede ser leves, graves o muy graves; el período de prescripción es de seis meses, dos años y tres, respectivamente. Como sujetos responsables de las mismas, el texto señala que serán responsables **tanto las personas físicas como jurídicas que realicen a título de dolo alguna de las infracciones contempladas** (y que, seguidamente se van a exponer). Como puede observarse, la **apreciación -o no- del *dolo* en los sujetos potencialmente responsable tiene una importancia crítica para esta norma,** puesto que, de no observarse, procede la exclusión de responsabilidad. Pues bien, para obtener una visión adecuada sobre la inferencia del dolo en el de contextos organizados, resulta absolutamente oportuno recomendar la lectura del report 6. Probabilidad del riesgo, dolo eventual e imprudencia consciente: examen de una difusa frontera entre la condena y la absolución de la persona jurídica.

Como **infracciones leves,** el Anteproyecto recoge: la remisión incompleta de información o fuera del plazo conferido (de manera dolosa) por parte del «responsable del sistema» a la Autoridad Independiente de Protección al informante; el incumplimiento de la obligación de colaboración con la investigación de informaciones (lo que podría situar a la corporación bajo la clásica -y ya referida- **disyuntiva deber colaboración vs. derecho a la potencial no autoincriminación con efectos en ulterior proceso penal)**; así como cualquier incumplimiento de las obligaciones previstas en esta ley que no esté tipificado como infracción muy grave o grave.

57. Composición: un representante del **Consejo de Transparencia y Buen Gobierno;** un representante de la **Oficina Independiente de Regulación y Supervisión de la Contratación;** un representante de la **Autoridad Independiente de Responsabilidad Fiscal;** un representante del Banco de España; un representante de la **CNMV;** un representante de la **CNMC;** un representante de **la Abogacía General del Estado**-Dirección del Servicio Jurídico del Estado; un representante de la **Oficina Nacional de Auditoría de la Intervención General** de la Administración del Estado; un representante del Ministerio de Hacienda y Función Pública perteneciente a la **Agencia Estatal de Administración Tributaria,** y dos representantes designados por el **Ministerio de Justicia** por un período de cinco años entre juristas de reconocida competencia con más de diez años de ejercicio profesional.

Asimismo, se contemplan seis grupos de conductas que tienen la consideración de infracciones muy graves y cinco que serán valoradas como graves:

Conductas muy graves

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

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

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

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

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

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

Conductas graves

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

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

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

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

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

Las SANCIONES PREVISTAS SON EXTRAORDINARIAMENTE CUANTIOSAS y, sin duda alguna, pueden causar un gravísimo quebranto a las personas jurídicas -o empresarios. De hecho, la norma prevé la imposición de las siguientes MULTAS[58]:

- **Si son PERSONAS JURÍDICAS** serán multadas con una cuantía hasta 100.000 euros en caso de infracciones leves, entre 100.001 y 600.000 euros en caso de infracciones graves y **entre 600.001 y 1.000.000 euros en caso de infracciones muy graves.**
- **Si son PERSONAS FÍSICAS** serán multadas con una cuantía de hasta 10.000 euros por la comisión de infracciones leves; de 5.001 hasta 30.000 euros por la comisión de infracciones graves y **de 30.001 hasta 300.000 euros por la comisión de infracciones muy graves.**

A este respecto, para **graduar las sanciones, se tendrán en consideración tanto la infracción como el contexto o circunstancias que concurran en cada caso.** Entre otros aspectos, se tendrán especialmente en cuenta factores como: la reincidencia; entidad del daño o perjuicio generado y su persistencia en el tiempo; intencionalidad y culpabilidad del autor (extremo que resulta algo confuso en tanto que el sujeto responsable ha de obrar, dolosamente[59], según la propia norma); el resultado del ejercicio anterior del infractor; la subsanación por propia iniciativa; reparación del daño causado y la colaboración con la Autoridad Independiente u otras autoridades administrativas.

En síntesis, como puede extraerse del conjunto de aspectos destacados en el presente *report 7*, el *Anteproyecto de Ley de Protección al Informante* vienen a imponer la adopción de «sistemas internos de información» y la dotación de un amplio elenco de mecanismos de protección a los informantes. A este respecto, las elevadísimas sanciones que se contemplan por incumplir sus disposiciones constituyen un importante estímulo fundado en el efecto disuasorio *(«deterret effect»)*.

Ahora bien, el lector habrá podido observar que, aunque los mecanismos y arquitectura orgánica que la norma exige a las organizaciones producirán efectos positivos en términos de capacidad para detectar incumplimientos, tras un análisis sosegado, también se aprecian ciertas inconsistencias, dificultades a la hora de armonizar sus preceptos con las exigencias de los «sistemas de compliance» y la existencia de varios puntos críticos con implicaciones jurídico-penales, tanto para el futuro «responsable del sistema interno de información» como para la propia defensa de la persona jurídica.

Rafael Aguilera Gordillo, Ph D
Codirector del Compliance Advisory LAB

Junio 2022

Web: Compliance Advisory LAB

58. Artículo 65 del Anteproyecto.

59. *«Artículo 62. Sujetos responsables.*

1. Estarán sujetos al régimen sancionador establecido en esta ley las personas físicas y jurídicas que realicen, a título de dolo, cualquiera de las actuaciones descritas como infracciones en el artículo 63.

2. Cuando la comisión de la infracción se atribuya a un órgano colegiado responderán de manera personal sus miembros en los términos que señale la resolución sancionadora. Quedarán exentos de responsabilidad aquellos miembros que no hayan asistido por causa justificada o que hayan votado en contra del acuerdo.

3. La exigencia de responsabilidades derivada de las infracciones tipificadas en la presente ley se extenderá a los responsables incluso aunque haya desaparecido su relación o cesado en su actividad en o con la entidad respectiva.»

Resumen

«Sistema Interno de Información»: La próxima -gran- obligación para toda persona jurídica o física con más de 49 trabajadores

Análisis de las ventajas, aspectos jurídico-penales, efectos sobre el sistema de compliance y otros puntos relevantes del Anteproyecto de Ley de Protección al Informante

Palabras clave: *compliance, sistema interno de información, canal de denuncias, responsable del sistema, investigación interna, compliance officer, protección al denunciante, sanciones, responsabilidad penal.*

Esta «futura ley» va a generar un **importantísimo cambio de paradigma** en la gestión de riesgos de las corporaciones españolas. El *Anteproyecto* contempla como **sujetos obligados del sector privado a cualquier empresario o persona jurídica que tenga más de 49 trabajadores.**

Por tanto, una parte muy importante de los agentes que conforman el tejido corporativo español tendrán que:

- **Adoptar «sistemas internos de información»**
- **Aplicar «mecanismos de protección al informante»**
- **Designar a un «responsable» del sistema interno de información**

Este séptimo *report* del **Compliance Advisory LAB** contiene un examen detallado del citado Anteproyecto.

El análisis comprende los **principales aspectos y ventajas** de la norma, **pero incluye el estudio de otras cuestiones de gran relevancia,** como las dificultades para compatibilizar su cumplimiento con las exigencias de los «*sistemas de compliance*» o la existencia de varios puntos críticos con implicaciones jurídico-penales, tanto para el futuro «responsable del sistema interno de información» como para la propia defensa de la persona jurídica (p.ej.: el acceso judicial al «libro-registro» de comunicaciones de la organización).

Entendemos que, solo desde este enfoque analítico integral, podrá obtenerse una **imagen más fiel y nítida de los efectos que la aprobación de esta norma pueden producir dentro de las organizaciones.**

El informe se divide en los seis epígrafes siguientes:

1. **«Finalidad de la ley y ámbito de aplicación»**
2. **«Sistemas internos de información» (y la figura del «responsable»)**
3. **«Canal externo de comunicaciones» y «disposiciones comunes» para canales internos y externos**
4. **«Revelación pública» y «protección de datos personales»**
5. **«Medidas de protección» de personas que comuniquen infracciones penales, comunitarias o administrativas que afecten al interés general y programas de clemencia.**
6. **«Autoridad Independiente de Protección del Informante» y «régimen sancionador»**

Se trata de un *report* que resulta de particular interés para **compliance officers, asesores legales corporativos, analistas de riesgos, órganos colegiados con funciones vinculadas al compliance y para los futuros responsables del denominado «sistema de información interna».**

Asimismo, dado que el incumplimiento de la norma conllevará la imposición de **sanciones de gran envergadura para el empresario o la persona jurídica (pueden alcanzar los 300.000€ para personas físicas y 1.000.000 en el caso de personas jurídicas),** el objeto de este informe concierne tanto a directivos como a miembros del consejo de administración.

Reports publicados

Consulta los reports publicados hasta la fecha por el Compiance Advisory Lab de Grant Thornton

REPORT 1

El «traslado» de responsabilidad penal entre empresas: Soporte socio-legal del artículo 130.2 C.P., identidad y due diligence penal.

REPORT 2

Refuerzo de la eficacia del Compliance: «Behavioral Compliance» y «Nudges».

REPORT 3

Incertidumbres en el Compliance Penal: fragilidades con implicaciones reales para la empresa. «Beneficio corporativo indirecto», «incumplimiento grave de los deberes de supervisión», «nulidad de prueba en investigaciones internas y confidencialidad».

REPORT 4

Consideraciones de profesionales expertos en Compliance: percepciones de especialistas del ámbito judicial, académico y empresarial sobre aspectos clave del Compliance.

REPORT 5

Tres Autos -cruciales- sobre compliance de la Audiencia Nacional: un análisis de los puntos clave de tres resoluciones judiciales dictadas en distintas investigaciones penales de relevancia que ilustran la especial trascendencia de los «sistemas de compliance».

REPORT 6

Probabilidad del riesgo, dolo eventual e imprudencia consciente: examen de una difusa frontera entre la condena y la absolución de la persona jurídica.

REPORT 7

«Sistema interno de información»: la próxima -gran- obligación para toda persona jurídica o física con más de 49 trabajadores. Análisis de las ventajas, aspectos jurídico-penales, efectos sobre el sistema de compliance y otros puntos relevantes del Anteproyecto de Ley de Protección al Informante.

Directores Compliance Advisory LAB

Fernando Lacasa

Socio de Forensic, Codirector del Compliance Advisory Lab

T +34 91 441 52 83

E Fernando.Lacasa@es.gt.com

Ver CV

Rafael Aguilera Gordillo

Codirector del Compliance Advisory LAB

T +34 91 576 39 99

E Rafael.Aguilera.ex@es.gt.com

Ver CV

https://www.grantthornton.es/servicios/financial-advisory/forensic/Compliance-advisory-lab/

www.grantthornton.es

Grant Thornton

grantthornton.es