JULIO 2023 | 15ª EDICIÓN
www.aeaecompliance.com/

EU Compliance news

UNA REVISTA DIRIGIDA A PROFESIONALES DESCÁRGALA AHORA

Potenciamos las capacidades de los especialistas en materia de Compliance para así reforzar de cara al exterior la imagen de calidad, solvencia y profesionalidad de todos los socios.

"FOMENTAR, COMPARTIR, DIFUNDIR Y FAVORECER EL DESARROLLO E IMPLANTACIÓN DE LA CULTURA DEL COMPLIANCE Y RESPONSABILIDAD SOCIAL."

ÍNDICE

ENTREVISTA. Katrin Meinke
Por Luis Suárez Mariño

El cambio cultural en las organizaciones requiere perseverancia y también personas y estructuras que lo impulsen. Por este motivo, la aportación de recursos humanos y financieros es esencial. Los procesos de cambio de este tipo no se ponen en marcha por sí solos.


PÁG.09

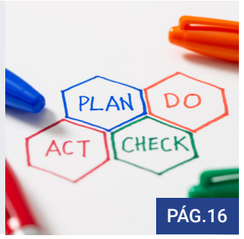

PÁG.12

ARTÍCULO. Ciberseguridad y Compliance
Por José Luis Colom Planas

En un mundo cada vez más interconectado e inmerso en la digitalización de la economía, la ciberseguridad ha dejado de ser una elección arbitraria de las organizaciones más cautas, para convertirse en un requisito de protección de los intereses y derechos de terceros, así como de la propia organización.

ARTÍCULO. ISO 37002:2021 Sistemas de gestión de la denuncia de irregularidades
Por Carlos Rozen

El futuro de la gestión de denuncias éticas es promisorio por su elevado poder de revelar la existencia y modalidad con la cual ocurren situaciones no deseadas, y considerando las tendencias emergentes, requerimientos legales y regulatorios, encuestas analizadas y los cambios en la cultura ética de las organizaciones.



PÁG.16


PÁG.22

ARTÍCULO. Corrupción, denuncias internas y algunas reflexiones en torno al sistema interno de información creado por la ley 2/2023 de 20 de febrero
Por Alejandro Cabaleiro

Desde una vertiente práctica, la nueva normativa ha establecido un nuevo sistema que deberá de convivir con la normativa derivada de los programas de cumplimiento normativo y con la obligación ex lege de puesta en conocimiento al Ministerio Fiscal de los hechos cuando indiciariamente se aprecien indicios de delito. Optando, desde una perspectiva subjetiva, por la conveniencia de que tal puesta en conocimiento sea pauta general y no excepción, a efectos de evitar problemas procesales y, puede, materiales, de incierta resolución.


PÁG.29

ARTÍCULO. Implicaciones de la ley de protección del anunciante en el derecho a no incriminase
Por Oliver Pascual Suaña

La obligación de informar al Ministerio Fiscal y la obligación de llevar un libro registro de las denuncias internas causa un claro peligro sobre el derecho a no incriminarse, al provocar que personas jurídicas que aparezcan como sujetos pasivos de un proceso penal se pueden ver compelidas a aportar documentos que contribuyan a su propia condena.

ARTÍCULO. Sobre el creciente uso de la IA en los ámbitos policial y judicial
Por Miguel Ángel Presno Linera

Algoritmos que aporten información de pronósticos para tomar decisiones que afecten a derechos se deben desarrollar como herramientas complementarias y de apoyo, para evitar caer en el «cum hoc ergo propter hoc».


PÁG.34


PÁG.37

ARTÍCULO. La teoria de los derechos etológicos y el Compliance
Por Oscar Germán Vázquez Asenjo

En el comportamiento etológico y por lo tanto también en el comportamiento Compliance no hay posibilidad de mantener actitudes pasivas, no es posible abstraerse de las circunstancias del mundo exterior. En este sentido, las consecuencias jurídicas no nacen de una relación querida y preestablecida con los demás, sino que lo hacen desde la pura acción que implica el comportamiento.

EMPRESA. Disfrimur: Apuesta por la descarbonización y el compromiso ético y social

Una empresa comprometida con sus clientes, con la sociedad y con su modelo de transporte, seguro, eficiente y sostenible.

PÁG.42


PÁG.44

REPERTORIO DE JURISPRUDENCIA
Por Manuel Montesdeoca de la Fuente

Principales sentencias del Tribunal Supremo y otros tribunales en materia de compliance y responsabilidad penal de las personas jurídicas.

DIRECTOR

Luis Suárez Mariño

CONSEJO EDITORIAL

Presidente:
Javier Bernabeu Aguilera

REDACCIÓN

Luis Suárez Mariño
Manuel Montesdeoca de la Fuente

EDITA

Asociación Europea de Abogados y Economistas en Compliance

GESTIÓN Y PUBLICIDAD

Neuromarketing Experiences S.L.

DOMICILIO SOCIAL

Passeig Mossen Jacint Verdaguer, 120, Entlo. 4ª
Igualada (Barcelona)

TELÉFONO

(+34) 938 049 038

CORREO ELECTRÓNICO

info@aeaecompliance.com

WEB

www.aeaecompliance.com

DISEÑO Y MAQUETACIÓN

Cristina Barrachina Vázquez

EUCompliance news

EDITORIAL

El pasado 13 de junio venció el plazo para que dentro del sector privado las empresas (personas físicas o jurídicas) que cuenten con 249 trabajadores o más, los partidos políticos, los sindicatos, las organizaciones empresariales y fundaciones creadas por unos y otros, tuvieran implantado un sistema interno de denuncias conforme a las exigencias de la **Ley 2/2023 reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción**, la cual incorpora al Derecho español la **Directiva (UE) 2019/1937 del Parlamento Europeo y del Consejo, de 23 de octubre de 2019** que regula aspectos mínimos que han de satisfacer los distintos cauces de información a través de los cuales una persona física que sea conocedora en un contexto laboral de una infracción del Derecho de la Unión Europea, pueda dar a conocer la existencia de la misma. En concreto, la Ley obliga a contar con canales internos de información a muchas empresas y entidades públicas porque se considera, y así también se ha recogido en informes y estadísticas recabados durante la elaboración del texto europeo, que es preferible que la información sobre prácticas irregulares se conozca por la propia organización para corregirlas o reparar lo antes posible los daños.

Por lo que se refiere al **objeto** de aplicación de la ley, la misma abarca no solo las infracciones del Derecho de la Unión previstas en la Directiva del Parlamento Europeo y del Consejo, sino que también se extiende a las infracciones penales y administrativas graves y muy graves de nuestro ordenamiento jurídico.

El **sistema interno de información,** que a partir del 1 de diciembre de este año obligará también a personas físicas y jurídicas que cuenten con 50 trabajadores o más, comprende, a tenor de la ley, entre los elementos que lo conforman, no solo un canal interno de información (la ley española ha preferido utilizar este término al de denuncia, y el de informante para referirse al denunciante, término que si utiliza la Directiva que transpone), sino que también debe contar con una **política o estrategia** que enuncie los principios generales en materia de sistemas interno de información y defensa del informante, un **procedimiento de gestión** de las informaciones recibidas que establezca las **garantías para la protección de los informantes en el ámbito de la propia entidad** y, por último, un **responsable del sistema** que, designado por el órgano de gobierno de cada entidad, desarrolle sus funciones de forma **independiente y autónoma** respecto del resto de los órganos de la entidad, sin recibir instrucciones de ningún tipo en su ejercicio y que disponga, además, de todos los **medios personales y materiales necesarios** para llevarlas a cabo.

Junto con estos cuatro elementos la ley impone además la obligación de **comunicar de forma clara y plenamente accesible a través de la home page de la web** de la entidad, en una sección separada y fácilmente identificable, el canal interno de información y las normas de uso del mismo, así como los principios esenciales del procedimiento de gestión de las informaciones recibidas y las garantías que la entidad se compromete a establecer a favor del informante; e igualmente exige la ley la **llevanza de un libro registro de las informaciones recibidas e investigaciones realizadas** preservando la confidencialidad y las normas de protección de datos.

Por lo que se refiere al **canal de comunicación** resulta conveniente insistir en, que conforme a la ley, las comunicaciones a través del Canal de Denuncias deberán de ser **trazables** (tener constancia fehaciente de cuándo y entre quiénes se produjeron), **protegidas** frente a posibles manipulaciones (que aseguren la invariabilidad de su contenido), y **garantizar la confidencialidad o anonimato del informante**, a fin de proteger de represalias al denunciante que alerta de posibles incumplimientos. Desde luego dichas exigencias no las cumple una mera cuenta de correo electrónico no exenta de riesgos de seguridad, como el phishing, el malware, el spam o correo no deseado o las fugas de información. Los correos electrónicos pueden contener información sensible o confidencial que, si es interceptada o divulgada por error, puede comprometer la privacidad y la seguridad de los individuos y sus datos personales vulnerando la confidencialidad de los mismos.

Es importante recalcar la importancia de generar un sistema interno de información que garantice la confianza, por parte de trabajadores, directivos y demás personas con acceso al canal de comunicación, en que la denuncia será tratada con la debida independencia y confidencialidad, sin temor a represalias.

Por otra parte, una política que enuncie los principios generales en materia de sistemas interno de información y defensa del informante, no se entiende sino en un contexto más general, dentro de una **Política general de compliance** o al menos de una política antifraude, incardinada en una cultura ética, entendida esta como aquella que nos auxilia a adoptar un comportamiento correcto ante un problema a la luz de las normas emanadas del poder legítimo del Estado y bajo el amparo del sistema constitucional; por eso la implantación de un sistema interno de información no debería limitarse a las concretas conductas incluidas en la Ley (a la denuncia de conductas presuntamente delictivas o constitutivas de infracciones graves o muy graves), sino que, en un contexto cultural de compliance, debería de incluir la denuncia de aquellas conductas que infringen las normas y procedimientos internos implantados en la organización como medios de prevenir precisamente dichas conductas delictivas o infractoras de las normas aplicables a la actividad desarrollada por la organización.

En este número de "European Compliance & News" se abordan algunas cuestiones de especial interés en relación con la ley 2/2023 reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción, y con su aplicación, como en qué medida la implantación de la ISO 37002:2021, Sistemas de Gestión de la denuncia de irregularidades, puede ser un instrumento útil en la aplicación de la ley; los requisitos de seguridad que ha de reunir el sistema para evitar ciberataques que puedan poner en riesgo la información contenida en el mismo y la confidencialidad de los datos; cómo ha de resolverse el posible conflicto que supone la obligación que impone la misma de trasladar al Ministerio Fiscal cualquier conducta que presente caracteres de delito con el derecho a no incriminarse de las personas jurídicas cuando la conducta presuntamente delictiva pudiera haberse cometido concurriendo los presupuestos para declarar también la responsabilidad penal de corporación, según el artículo 31 bis del Código Penal, o los supuestos en que la confidencialidad del denunciante puede quedar expuesta en sede judicial.

Algunos de estos problemas ya se han planteado en la práctica. El 4 de julio la Sala Tercera de la Sala Contencioso-Administrativo del Tribunal Supremo celebraba la vista pública del recurso de casación contra una sentencia dictada por el Tribunal Superior de Justicia de la Comunitat Valenciana que anulaba la protección de una persona denunciante de corrupción realizada por la Agencia Valenciana Antifraude. En el Auto de admisión del recurso la Sala declara que la cuestión planteada en el recurso que presenta interés casacional objetivo para la formación de la jurisprudencia consiste en determinar si resulta aplicable 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, cuando esta no había sido todavía traspuesta en plazo, y ello con independencia de su invocación en la instancia y, para el caso de que la respuesta a la cuestión anterior sea afirmativa, las consecuencias que de ello se derivan en el caso concreto enjuiciado, lo que a tenor del recurso planteado supone determinar si la protección a la persona denunciante se ha de ofrecer con independencia del canal por el que se efectúe la denuncia, es decir, con independencia de si es un canal interno de denuncias, externo o judicial.

Otros problemas que plantea la aplicación de la Ley 2/2023 también fueron tratados por expertos en la Jornada de compliance organizada por la AEAEC, Fundación Corell, Alsa y CMC XXI, de la que damos cuenta en este número de la revista.

Junto con estos temas, son objeto de estudio, el creciente uso de la inteligencia artificial en los ámbitos policial y judicial que acabamos de vivir y los efectos potencialmente importantes para la democracia, el Estado de Derecho, las libertades individuales y el derecho a la tutela judicial efectiva y a un juez imparcial, **o las posibles utilidades que para la figura del Compliance puede ofrecer su consideración dentro de la novedosa teoría de los derechos etológicos.**

En fin, no queremos terminar sin desear suerte al legislador y al gobierno que se conforme, tras el proceso electoral que acabamos de vivir, confiando en que en esta legislatura siga avanzando en nuestro país el compromiso de las administraciones con el compliance y la cultura ética y de cumplimiento.

JORNADA "NUEVOS RETOS EN MATERIA DE COMPLIANCE"

El pasado viernes 12 de mayo tuvo lugar en el auditorio GMP, Madrid, la Jornada **"Nuevos Retos en materia de compliance" organizada por la Fundación Corell, Alsa, CMC XXI y la Asociación de abogados y economistas en compliance** a la que asistieron presencialmente además de los presidentes de la Fundaciónn Corell, don Marcos Basante y de la AEAC, don Javier Bernabéu, y el consejero de Lenovo y el consejero delegado de ALSA, don Francisco Iglesias mas setenta profesionales, entre directivos, oficiales de cumplimiento, profesores universitarios, abogados y auditores.

La jornada que fue transmitida en streaming, fue presentada por **Don Marcos Basante Fernández**, recién elegido presidente de la Fundación Corell, el cual dejó constancia del compromiso de la Fundación con la cultura de cumplimiento y de la importancia que en materia de compliance tienen la comunicación y formación.

La **primera ponencia, que versó sobre la responsabilidad penal de administradores y directivos corrió a cargo de don Antonio del Moral,** magistrado de la sala II, de lo penal, del Tribunal Supremo, qué de manera muy ilustrativa y práctica, puso de manifiesto la tragedia que supone para un administrador o directivo, y en general para cualquier persona, el sometimiento a un proceso penal; la famosa pena de banquillo. "La tragedia del proceso penal es no poder saber si el investigado será o no sancionado" afirmó, y utilizando palabras muy expresivas de Carnelutti incidió en la idea de que "toda sentencia absolutoria es un error judicial".

"LA TRAGEDIA DEL PROCESO PENAL ES NO PODER SABER SI EL INVESTIGADO SERÁ O NO SANCIONADO"

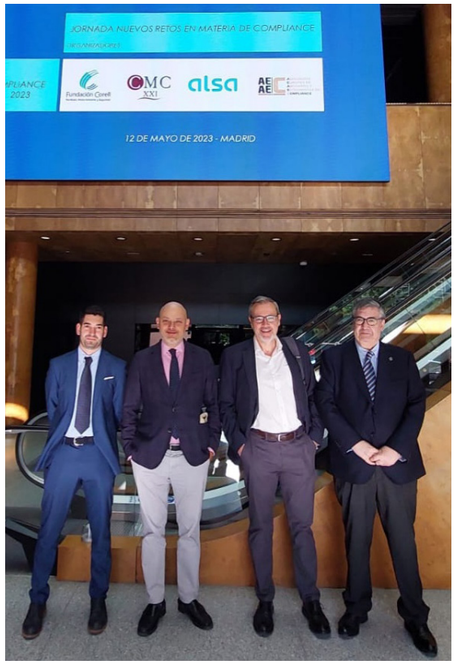
Partiendo de esta idea, del Moral explicó como el ámbito objetivo del derecho penal se extiende y amplia cada día más para la empresa y sus directivos, siendo también cada día más difícil deslindar la frontera entre lo punible y lo no punible, hasta el punto de que se puede hablar de "fronteras vaporosas" entre lo delictual y lo no delictual.

En cuanto la responsabilidad penal del oficial de cumplimiento trajo a colación el magistrado el art. 11 del C.P. haciendo hincapié en la necesidad de que para que exista responsabilidad penal es necesario que concurra no solo la posición de garante, sino la posibilidad de cometer el delito por comisión por omisión - lo que implica en los delitos que consistan en la producción de un resultado, que la no evitación del mismo, al infringir un especial deber jurídico del autor, equivalga a su causación- y una prueba al menos indiciaria suficiente para condenar penalmente al oficial de cumplimiento, subrayando del Moral, que la omisión del deber de denunciar un injusto solo se castiga cuando el delito es un delito continuado cuya no denuncia puede conllevar que el mismo se siga cometiendo en la organización.

Seguidamente tuvo lugar una **mesa redonda sobre el compliance y el derecho de la competencia y el impacto de la actuación del CNMC en la empresa, a cargo de don Miguel de los Santos Gandarillas Martos**, magistrado de la sala de lo contencioso-administrativo de la Audiencia Nacional y **doña Paloma Martínez-Lage Sobredo,** socia de Baker McKenzie especializada en competencia y compliance.

Ambos ponentes pusieron de manifiesto el impulso definitivo de las políticas de cumplimiento normativo en el ámbito de las normas de defensa de la competencia, avance propiciado de la mano de dos importantes novedades legislativas: la prohibición de contratar con las administraciones públicas que se impone al empresario sancionado por infracciones graves de la Ley de Defensa de la Competencia y la Directiva del Parlamento Europeo y del Consejo, relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión, conocida también como "Directiva *Whistleblowing*".

En lo que se refiere a las sanciones impuestas por la CNMC, los ponentes pusieron en común su experiencia tanto en relación a la posibilidad de imponer sanciones a los representantes legales y directivos que hayan participado en los acuerdos anticompetitivos detectados, como en relación a las consecuencias que pueden derivarse de una sanción firme por infracción de la LDC en el ámbito de la contratación pública, así como, finalmente, en el posible ejercicio por las víctimas de infracciones de las normas de competencia de acciones de responsabilidad por los daños y perjuicios



De izquierda a derecha: Andrés R.Huesca, Manuel Montesdeoca, Luis Suárez, José Félix R. Busto.

ocasionados, sobre todo tras la transposición de la conocida como Directiva de daños.

En relación a la eficacia de los programas de cumplimiento como medio de minimizar las sanciones conforme a la atenuación de su responsabilidad derivada del programa de cumplimiento, estuvieron de acuerdo los ponentes en incidir en el hecho de que la CNMC solo da relevancia a los programas cuando la aplicación de los mismos ha conllevado consecuencias disciplinarias para los autores de la infracción, mientras que, en los demás casos, la CNMC no da ningún trato favorable a las empresas que comenten actos sancionables con el argumento de que el mero hecho de introducir estos programas internos de adecuación a las normas sobre competencia no puede tomarse sin más como una circunstancia atenuante, sobre todo en los casos en los que la acreditación de una infracción es una evidencia clara para las empresas sancionadas de un fallo en el cumplimiento de tales normas internas.

Igualmente los ponentes fueron críticos con la actividad sancionadora de la CNMC en relación a la constitución de Uniones Temporales de Empresas UTES, "que muchas veces son urdidas por la propia Administración contratante" y afirmaron que con harta frecuencia la CNMC las considera ilegales con el apriorístico argumento de que son utilizadas como un instrumento para repartirse las licitaciones públicas convocadas por la Administración, y no existir justificación objetiva económico-financiera, tecnológica o falta de capacidad para atender en plazo las exigencias de la licitación. Argumento, señaló de los Santos, del que en no pocas ocasiones discrepa por vía de recurso la Audiencia Nacional, criticando que en muchas de las resoluciones de la CNMC se hecha falta de un mínimo estándar probatorio y argumentativo para justificar una infracción, no teniendo en cuenta que la potestad sancionadora no puede llegar al extremo de interferir en la libertad de empresa marcando opciones de indudable carácter empresarial.

"LA POTESTAD SANCIONADORA NO PUEDE LLEGAR AL EXTREMO DE INTERFERIR EN LA LIBERTAD DE EMPRESA MARCANDO OPCIONES DE INDUDABLE CARÁCTER EMPRESARIAL".

María Massó durante su intervención

La última mesa redonda protagonizada por don Alejandro Abascal Junquera, magistrado en el Juzgado Central de instrucción nº 1 de la Audiencia Nacional **y doña María Massó Moreu**, especialista en compliance e investigaciones internas en Baker McKenzie, versó **sobre las últimas sentencias del Tribunal Supremo y la Audiencia Nacional y las obligaciones y desafíos ante la Ley 2/2023.**

Comenzó Abascal desgranando las últimas sentencias del Supremo en relación a la valoración de los programas de cumplimiento tanto en lo que respecta a la responsabilidad penal de las personas jurídicas como a la responsabilidad civil subsidiaria de estas. Subrayó Abascal los efectos beneficiosos de los programas de compliance ad intra, que permiten reducir o evitar, según el Supremo, la denominada "autopuesta en peligro".

Insistió el magistrado en que resulta evidente, y así es reconocido por el Supremo, que los programas de compliance reducen el riesgo de actividades delictivas aún de aquellas, respecto de las cuales el legislador no ha considerado oportuno incluir entre las conductas de las cuales puede derivarse responsabilidad penal para la persona jurídica. Por ello, concluyó el magistrado "No tener hoy en día un buen programa de compliance resulta inaudito".

"NO TENER HOY EN DÍA UN BUEN PROGRAMA DE COMPLIANCE RESULTA INAUDITO"

También valoró el magistrado los elementos necesarios que ha de reunir un programa de prevención de riesgos penales, tema en el que la Audiencia Nacional, tanto la sala de lo penal como los juzgados de instrucción, han tenido mayor oportunidad para pronunciarse, subrayando que "más allá de la concurrencia de los concretos elementos que establece el art. 31 bis 5 del C.P. conformadores del programa de prevención de delitos, y presuponiendo la existencia de los mismos, se ha de valorar particularmente si la persona jurídica actualiza los riesgos penales y demás elementos de su programa, así como los procesos de diligencia debida que la misma emplea y los recursos humanos y económicos que emplea en su aplicación".

Por su parte Massó se ocupó de los aspectos más controvertidos y necesarios de interpretación de la reciente Ley 2/2023 reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción, conocida como "Ley Whistleblowing".

Paloma Martínez-Lage y Miguel de los Santos Gandarillas

En relación al sector privado, se mostró Massó partidaria de la posibilidad de externalizar tanto la gestión del sistema de recepción de las informaciones, como de externalizar también, si se ve oportuno, las investigaciones internas a que de lugar la información, sin perjuicio de la responsabilidad del sistema que compete tanto al responsable del mismo como como al órgano de gobierno que lo nombra.

Igualmente invitó la letrada, experta en investigaciones internas, a distinguir el ámbito de las investigaciones a que pueda dar lugar el sistema interno de información, de otras investigaciones que pueden tener lugar en el seno de la empresa a consecuencia de una auditoría interna o un procedimiento de investigación penal.

Según la ley, el Sistema interno de información, subrayó Massó, deberá estar diseñado, establecido y gestionado de forma segura, y garantizar la confidencialidad de la identidad del informante, de la persona afectada por la información y de cualquier tercero mencionado en la comunicación, impidiendo el acceso de personal no autorizado.

Alejandro Abascal durante su intervención

Por lo que respecta a la externalización de la gestión del sistema interno de información en entes del sector público, incidió Massó en que la ley solo permite la misma cuando el ente acredite la insuficiencia de medios propios y además en ese caso limitando la externalización al instrumento, la plataforma o aplicación informática a través de la cual se remitiera la información.

También subrayó la letrada el impacto que tendrá la Ley en la contratación del sector público y, en especial, sobre los contratistas y subcontratistas que operan en el mismo. Con la entrada en vigor de la Ley las empresas que operan en el sector público se enfrentan a un mayor

De izquierda a derecha: Luis Suárez, Javiér Bernabéu, Alejandro Samper, Victor Tartiere, Alejandro Abascal, Paloma Martínez-Lage, Miguel de los Santos Gandarillas, María Massó y Marcos Basante.

riesgo, pues sus eventuales infracciones pueden quedar más fácilmente al descubierto y ser objeto de sanciones, desde la resolución del contrato por incumplimiento culpable o la prohibición de contratar.

"CON LA ENTRADA EN VIGOR DE LA LEY, LAS EMPRESAS QUE OPERAN EN EL SECTOR PÚBLICO SE ENFRENTAN A UN MAYOR RIESGO, PUES SUS EVENTUALES INFRACCIONES PUEDEN QUEDAR MÁS FÁCILMENTE AL DESCUBIERTO Y SER OBJETO DE SANCIONES"

Analizaron también los ponentes las tensiones existentes en cuanto a la obligación de atender determinados requerimientos de la Autoridad independiente de protección del informante o la obligación de remitir con carácter inmediato al Ministerio Fiscal informaciones de hechos que indiciariamente pudieran ser constitutivos de delito y el derecho a la no incriminación de la persona jurídica, concluyendo que deberá de ser una cuestión a valorar por la empresa, atendiendo a las consecuencias que se pudiera derivar para la persona jurídica, en uno y otro caso, si resulta menos lesivo remitir o no la información a las autoridades, teniendo en cuenta que el procedimiento penal en definitiva siempre resulta ser más garantista que el administrativo sancionador.

Tras un intenso debate entre los ponentes y los asistentes, **clausuró la jornada** por don **Victor Tartiere,** miembro del comité de cumplimiento de Alsa y Fundación Corell, y delegado de la AEAEC en Asturias, dando las gracias a ponentes y asistentes e invitando a los mismos a un vino español.

Acceso a la grabación de la Jornada:

YouTube **Reproducir video**

ENTREVISTA A KATRIN MEINKE

Por Luis Suárez Mariño
Director de European Compliance News

Periodista, licenciada en literatura alemana y española en la TU Berlín. Desde 2012, dirije el centro de apoyo a las familias de Humboldt-Universität zu Berlin.

Ante el convencimiento de que el clima y la cultura organizacional se demuestran influyentes en la conducta de las personas y que *clima de atención y cuidado,* está relacionado con la satisfacción de las personas y con un bajo comportamiento disfuncional como han puesto en evidencia algunos estudios, nos hemos ido hasta Berlín para conocer de la mano de Katrin Meinke, responsable del centro de apoyo a la familia de la Humboldt-Universität de Berlín, los resultados que la Universidad ha obtenido desde que ha adoptado como objetivo estratégico constituirse en un entorno familiar que tiene como misión favorecer la igualdad de oportunidades y posibilitar la participación de todos los miembros de la comunidad universitaria, la compatibilidad entre carrera, estudios, cualificaciones y familia mediante la institucionalización de las estructuras de implementación necesarias, la adopción de medidas concretas y la dedicación de recursos al proceso, que es certificado por una auditoría externa 'Audit familiengerechte hochschule' (Auditoría universitaria favorable a la familia), que evalúa los requisitos y la idoneidad de las medidas adoptadas estas medidas.

Buenos días Katrin, muchísimas gracias por recibirnos. Como sabes a través de "European Compliance & News"procuramos fomentar la cultura ética en las organizaciones. Sabemos por estudios psico-sociales que el clima y la cultura organizacional se han demostrado influyentes en la conducta de las personas que conforman la misma y que un *clima de atención y cuidado de las personas y su entorno familiar está relacionado con la satisfacción y la cultura ética.*

Desde este punto de vista **¿se puede inscribir el esfuerzo que hace la Universidad Humboldt-Universität de Berlin por integrar el bienestar familiar de trabajadores, profesores, estudiantes, en la cultura de la universidad?**

Sí, por supuesto. Es bien sabido que las medidas para mejorar la compatibilidad entre trabajo, estudio y familia tienen un efecto positivo en el clima laboral y de estudio, lo que a su vez redunda en mejores resultados.

¿Cuál fue la génesis de esta cultura de integración de la vida familiar, educativa y profesional que se lleva a cabo en la HU?

En 2009, la Humboldt-Universität zu Berlin asumió su primer compromiso para fomentar la compatibilidad entre trabajo, estudios y familia con una auditoría, con la que se han puesto en marcha varias medidas importantes. Por ejemplo, la creación de una oficina de la familia como punto central de organización y servicios, la inclusión del objetivo de conciliar trabajo, estudios y familia en la constitución de la Universidad,, la posibilidad de flexibilizar los estudios por motivos familiares y la oferta de cuidado de niños para miembros de la universidad. Hitos del proceso de auditoría son el establecimiento de una guardería y de normas sobre compensación de desventajas en el reglamento de estudios.

¿Cuáles son los valores que la inspiran?

Los valores subyacentes se establecen en la constitución de la Humboldt-Universität zu Berlin: El objetivo de la universidad es cumplir su obligación social además de su mandato legal. Esto incluye la eliminación de las desventajas existentes para las mujeres, la inclusión de todos los miembros de la universidad con especial consideración a las necesidades de las personas con discapacidad o enfermedad crónica, la superación de las desventajas estructurales basadas en la discriminación basada en el origen social o étnico y la compatibilidad de los estudios, el trabajo y la familia.

¿Cuáles son los objetivos de esta cultura de integración?

Los esfuerzos de la HU en estos ámbitos sirven para promover la igualdad de oportunidades y para que todos los miembros

de la universidad puedan participar en la vida universitaria.

¿Cuáles son los programas para conseguir los objetivos propuestos?

Por ejemplo, la Universidad se compromete a establecer una infraestructura favorable a las familias. Esto incluye salas para padres e hijos e instalaciones para cambiar pañales, oportunidades de asesoramiento y creación de redes e información exhaustiva para todos los miembros de la universidad.

La flexibilidad es un componente necesario de una universidad favorable a las familias. Teniendo esto en cuenta, la Universidad ofrece a sus empleados y estudiantes una variedad de opciones: Entre ellas se incluyen horarios de trabajo y estudio adaptados a la familia, así como el trabajo móvil y cursos online. Se anima a los supervisores y profesores a encontrar soluciones flexibles en casos individuales para conciliar el trabajo, los estudios y la vida familiar.

¿Hacéis desde la Humboldt-Universität un seguimiento de los resultados obtenidos?

Los objetivos y las medidas se someten a una evaluación y auditoría periódica para seguir desarrollándolos continuamente.

¿El éxito de esa cultura de integración parte de un concepto abierto de familia?

Sí, efectivamente. La Humboldt-Universität concibe la familia como cualquier comunidad de personas en la que se asume una responsabilidad social a largo plazo. Por lo tanto se incluyen todas las comunidades de padres e hijos - incluidas las familias con padres o madres solteros o del mismos sexo y las familias patchwork -, pero también las relaciones entre hermanos, así como el matrimonio y las uniones similares al matrimonio.

¿Puedes ahondar un poco en la experiencia que tenéis en relación con la integración de familias de procedencias culturales, religiosas e ideológicas distintas, algunas de las cuales son, al menos aparentemente, no respetuosas con el derecho de igualdad y las libertades individuales?

La universidad es un punto de encuentro extremadamente internacional. Se reúnen personas de diferentes culturas, religiones y también ideologías. Ciertamente, esto puede llevar a conflictos y diferencias, pero no entran en juego en mi trabajo personal. Lo que más me preocupa son los conflictos entre directivos y empleados o entre profesores y estudiantes que resultan de expectativas diferentes en cuanto a la conciliación de la vida universitaria y familiar, independientemente del origen cultural o religioso de las personas.

En relación con esto que dices, ¿qué resultados ha tenido la implementación de esa política de integración en la mejora del clima universitario y la reducción de conflictos o tratos discriminatorios?

Las encuestas a empleados y estudiantes muestran que esta política de integración tiene un efecto positivo en el clima universitario. Estoy convencida de que hoy en día las necesidades de las personas con responsabilidades familiares se tienen mucho más en cuenta en la Humboldt-Universität que hace diez años. Por supuesto, los conflictos no pueden evitarse por completo, pero los afectados tienen un soporte patente en el centro de apoyo a las familias.

¿La Humboldt-Universität se preocupa por incorporar los valores del estado democrático y el respeto a los derechos de los demás a las familias de profesores o alumnos refugiados de distintas culturas, religiones o ideologías? ¿Cómo lo hace?

Sí existen varios programas para empleados y estudiantes internacionales en la universidad. También hay programas especiales para refugiados. Estos programas se centran en la ayuda para la integración, por ejemplo mediante servicios de asesoramiento en inglés o el apoyo en acudir a las autoridades, como la Oficina de Registro de Extranjeros.

Desde tu experiencia. ¿En que medida la cultura de las organizaciones necesita ser institucionalizada a través de la creación de estructuras de implementación y dotada de recursos financieros y humanos adecuados?

En efecto, el cambio cultural en las organizaciones requiere perseverancia y también personas y estructuras que lo impulsen. Por este motivo, la aportación de recursos humanos y financieros es esencial. Los procesos de cambio de este tipo no se ponen en marcha por sí solos.

Muchas gracias, Katrin, ha sido muy enriquecedor hablar contigo y que nos compartas tu experiencia, espero que los buenos resultados alcanzados en la Universidad Humboldt con esta política y cultura de integración sirvan de inspiración a muchas otras organizaciones, desde el convencimiento de que un clima de atención y cuidado de las personas y su entorno familiar está relacionado con la satisfacción y la cultura ética en las organizaciones.

CIBERSEGURIDAD Y COMPLIANCE

José Luis Colom Planas

Asesor del Centro Criptológico Nacional (CCN)

En un mundo cada vez más interconectado e inmerso en la digitalización de la economía, la ciberseguridad ha dejado de ser una elección arbitraria de las organizaciones más cautas, para convertirse en un requisito de protección de los intereses y derechos de terceros, así como de la propia organización.

Los marcos normativos, ya sean jurídicos, como el Esquema Nacional de Seguridad (ENS) regulado por el RD 311/2022, de 3 de mayo, o de adscripción voluntaria, como la norma ISO/IEC 27001:2022 sobre sistemas de gestión de seguridad de la información (SGSI), son un facilitador más para garantizar el cumplimiento de las organizaciones.

En este sentido, el Corporate Compliance Officer (CCO), u Oficial de Cumplimiento como lo designamos en España, debe implicarse en la consideración de la Ciberseguridad por parte de la Organización en la que presta su desempeño profesional.

ALGUNAS DEFINICIONES PARA ACLARAR CONCEPTOS

Podemos considerar el **CIBERESPACIO** como aquel espacio virtual, constituido por medios cibernéticos (TIC), donde se agrupan los diferentes servicios digitales de Internet.

En consecuencia, entenderemos por **CIBERSEGURIDAD** la protección de los Sistemas de Información que se encuentran conectados al ciberespacio de los potenciales ataques procedentes de Internet, preservando así los servicios que prestan y la información que manejan.

Podemos ver la Ciberseguridad como un subconjunto de un concepto más amplio, que es la SEGURIDAD DE LA INFORMACIÓN. A modo de ejemplo aclaratorio, la Ciberseguridad no abarca la protección ante una intrusión física a un Centro de Datos, ni ante la inserción de un pendrive USB infectado con malware en un equipo informático, ataques que sí se contemplan desde el punto de vista más amplio de la seguridad de la información y/o de los servicios.

De la definición de Ciberseguridad surge la necesidad de clarificar que se entiende por un Sistema de Información, a diferencia de un sistema informático. Entendemos por **SISTEMA DE INFORMACIÓN** aquel conjunto de elementos, habitualmente tecnológicos (sistemas informáticos y de comunicaciones) pero que suelen incluir personas, que interactúan para soportar los servicios que dicho sistema presta, tratando la información que éstos manejan. Como vemos, pone el acento en lo material, es decir, personas y tecnología.

Adicionalmente, respecto a un Sistema de Información se pueden implementar **SISTEMAS DE GESTIÓN**, que podemos definir como un conjunto de instrumentos organizativos (Políticas, normas internas, procedimientos, etc.) interrelacionados y orientados a mejorar la eficacia y la eficiencia de lo gestionado. En el caso de un Sistema de Gestión de la Seguridad de la Información (SGSI) se pretende mejorar la eficacia y la eficiencia de la seguridad del Sistema de Información sobre el que se aplica.

Otros Sistemas de Gestión son, por ejemplo, de calidad, que determina la norma ISO 9001:2015, ambiental, basado en la norma ISO 14001:2015, de Compliance, que determina la norma ISO 37301:2021, etc.

Para finalizar este elenco de definiciones, definiremos S**EGURIDAD DE LA INFORMACIÓN**, en sentido amplio, como el conjunto de medidas preventivas (basadas en el riesgo) y reactivas, que permiten proteger en todas las dimensiones establecidas los servicios y la información, junto a los demás activos vinculados, que constituyen un Sistema de Información.

La seguridad es un término abstracto que para ayudar a perfilar habitualmente se descompone en tres dimensiones: la Confidencialidad, la Integridad y la Disponibilidad, aunque el ENS considera adicionalmente la Autenticidad y la Trazabilidad, hasta totalizar cinco dimensiones, según señala el apartado 2 del Anexo I del RD 311/2022, señalando: *"A fin de determinar el impacto que tendría sobre la organización un incidente que afectara a la seguridad de la información tratada o de los servicios prestados y, en su consecuencia, establecer la categoría de seguridad del sistema de información en cuestión, se tendrán en cuenta las siguientes dimensiones de la seguridad, que se identificarán por sus correspondientes iniciales en mayúsculas: a) Confidencialidad [C]; b) Integridad [I]; c) Trazabilidad [T]; d) Autenticidad [A]; e) Disponibilidad [D]"*.

Podemos definirlas por la finalidad que pretenden:

- **Confidencialidad:** Garantiza que la información únicamente será accesible a quienes están autorizados a hacerlo.
- **Integridad:** Garantiza que la información únicamente será modificada por quienes tienen autorización para hacerlo.
- **Disponibilidad:** Garantiza que la información y los servicios estén disponibles durante los intervalos establecidos.
- **Autenticidad:** Garantiza que quién accede o proporciona información realmente "sea quién dice ser".
- **Trazabilidad:** Garantiza que en todo momento pueda conocerse "quién hizo qué".

LOS ESLABONES MÁS DÉBILES DE LA CADENA

Si asimilamos una organización a una cadena, los eslabones más débiles desde el punto de vista de la Ciberseguridad suelen ser los **empleados y colaboradores**. Los ciberdelincuentes lo saben y por esta razón intentarán romper primero esos eslabones, previendo que así obtendrán un ahorro en el esfuerzo necesario para comprometer la Organización.

Un ejemplo lo tenemos en los Ciberataques basados en técnicas de ingeniería social como puede ser el phishing, la suplantación de identidad, etc.

Es por dicho motivo que, además de las medidas de seguridad técnicas y organizativas, las acciones directas focalizando en empleados y colaboradores, como lo es la concienciación en Ciberseguridad, se tornan en imprescindibles.

Pero, desde un punto de vista riguroso, ¿Qué diferencia hay entre formación y concienciación? Quienes tengan formación jurídica están en mejores condiciones para comprender la diferencia inicialmente, ya que una distinción doctrinal en la Teoría del Derecho determina que una norma pude descomponerse en reglas y principios.

Las REGLAS indican lo que debe o no debe hacerse, mientras que los PRINCIPIOS son aquel bien superior que justifica las reglas. Ante esta tesitura, podemos entender que mientras la Formación se limita a explicar las reglas a las personas, haciéndolo de la forma más didáctica posible, la Concienciación supone determinadas acciones encaminadas a favorecer que las personas interioricen los principios, de modo que no incumplan las reglas, tanto si se sienten observadas, como si no.

En consecuencia, un equilibrio entre **formación y concienciación** parece la fórmula adecuada. En este sentido, el ENS dispone de dos medias de seguridad específicas en su Anexo II:

De una parte, la medida **[mp.per.3] Concienciación,** que señala *"Se realizarán las acciones necesarias para concienciar regularmente al personal acerca de su papel y responsabilidad para que la seguridad del sistema alcance los niveles exigidos. En particular, se recordará periódicamente:*

- *[mp.per.3.1] La normativa de seguridad relativa al buen uso de los equipos o sistemas y las técnicas de ingeniería social más habituales.*
- *[mp.per.3.2] La identificación de incidentes, actividades o comportamientos sospechosos que deban ser reportados para su tratamiento por personal especializado.*
- *[mp.per.3.3] El procedimiento para informar sobre incidentes de seguridad, sean reales o falsas alarmas".*

De otra parte, la medida **[mp.per.4] Formación,** que señala:

- *"[mp.per.4.1] Se formará regularmente al personal en aquellas materias relativas a seguridad de la información que requiera el desempeño de sus funciones, en particular en lo relativo a:*
  - *Configuración de sistemas.*
  - *Detección y reacción ante incidentes.*
  - *Gestión de la información en cualquier soporte en el que se encuentre. Se cubrirán al menos las siguientes actividades: almacenamiento, transferencia, copias, distribución y destrucción.*
- *Además, se evaluará la eficacia de las acciones formativas llevadas a cabo".*

CONCLUSIONES INFERIDAS OBSERVANDO CIBERATAQUES

Existe una gran variedad de posibles ciberataques, ciberdelitos si se prefiere, con implicaciones directas o indirectas en la Organización que se producen constantemente.

Entre todos ellos, cabe citar: Código dañino (malware) en general; Ransomware, en particular, con exfiltración previa de datos sensibles para asegurar la extorsión, junto a cifrado masivo la información; ataques basados en ingeniería social, como lo son:

- El phishing, ya sea masivo o dirigido;
- La suplantación de identidad haciéndose pasar, por ejemplo, por un proveedor que desea cambiar la cuenta bancaria donde recibir las transferencias;

- El fraude del CEO, haciéndose pasar el ciberdelincuente por el CEO de la organización para ordenar un pago de forma urgente, necesario para cerrar un 'negocio' sin tiempo a verificarlo por el personal administrativo;

- Ataques de denegación de servicio, impidiendo los accesos legítimos a determinado portal web;

- Espionaje e intrusiones a los servidores de una Organización para acceder a información sensible, alterarla o suprimirla;

- Hacktivismo para causar daños a la Organización atacada, tal vez a su imagen; etc.

Desgraciadamente, podemos llegar a afirmar que todas las organizaciones, ya sean del sector público o privado, deben considerar que **no se trata de "si se producirá" un ciberataque, sino de "cuándo se producirá" y si cuando eso ocurra, la organización estará preparada.** Por lo tanto, todas las organizaciones deben revisar, actualizar y reforzar continuamente la ciberseguridad.

Un ciberataque puede tener consecuencias muy graves, tanto en términos de posible interrupción de las operaciones, como por el daño reputacional y/o económico que pueda causarse a empleados, clientes, etc.

Al final, puede llegar a afirmarse que la seguridad de la información en la 'era digital' es una de las aristas de la **sostenibilidad,** ya que 'nadie usa aquello en lo que no confía'.

EL CONCEPTO DE COMPLIANCE Y SU RELACIÓN CON LA CIBERSEGURIDAD

Según la norma ISO 37301:2021, *"Compliance es un proceso continuo y el resultado de que una organización cumpla con sus obligaciones"*.

En esta definición de amplio recorrido cabe todo. Es por ello que cobra valor una buena definición del 'alcance', es decir, de los límites que determinan el ámbito que abarcará el Sistema de Gestión de Compliance (SGC) que se defina e implante en la Organización.

En consecuencia, podemos hablar de Compliance en general; de Compliance legal, si lo circunscribimos al cumplimiento de las obligaciones legales que marca el ordenamiento jurídico de la(s) jurisdicción(es) donde opera la Organización; de Compliance Penal, si pretendemos llegar a impedir que se cometan delitos en nombre o por cuenta de la Organización y en su beneficio, pudiendo, consecuentemente, quedar exonerada de responsabilidad penal la persona jurídica que implante eficazmente, por ejemplo, en España, un SGC basado en la norma UNE 19601:2017; y, por último, de Compliance respecto a las obligaciones como sujeto obligado que determina la Ley 10/2010 de PBCyFT. Y así podríamos continuar determinando otras parcelas de cumplimiento.

Podemos analizar las implicaciones en Compliance, es decir, en el cumplimiento o incumplimiento de las obligaciones por parte de una Organización, partiendo de las consecuencias del ciberataque que, en muchas ocasiones, impedirán cumplir:

- **Exfiltración de información:** incumplimiento de cláusulas contractuales y/o acuerdos de confidencialidad.

- **Violaciones de datos personales:** incumplimiento de la responsabilidad de custodiar datos personales de empleados, clientes (ciudadanos en el sector público) y proveedores. Violación según la determina el art. 33 RGPD.

- **Pérdida de continuidad del negocio:** incumplimiento contractual debido a la pérdida de disponibilidad en los servicios, derivando en reclamaciones de clientes. Incumplimiento de preceptos legales debido, por ejemplo, a la incapacidad de atender al ejercicio de derechos de Protección de Datos.

- **Daño reputacional:** A la organización que ha sufrido el ciberataque y/o al honor y a la propia imagen de terceros.

- **Daños a terceros:** Ordenadores zombis que han sido hackeados para obedecer a un puesto de mando y control y lanzar desde él ataques a terceros, por ejemplo, de denegación de servicio (DoS o DDoS).

- **Pasarela para acceder a un tercero:** Hackeo de una Organización para, desde ella, entrar y comprometer a sus clientes.

- **Etc.**

La responsabilidad de la Persona Jurídica (PJ) puede ser de diferente naturaleza, como penal o civil.

La PJ autora del ciberataque puede incurrir en:

- **Responsabilidad penal derivada de la comisión de dos posibles delitos:** el primero, de daños informáticos (art. 264 CP), y el segundo, de descubrimiento de secretos o vulneración de la intimidad (art. 197 al 200 CP).

- **Responsabilidad civil subsidiaria,** tipificada en el art. 120.4 CP.

La PJ atacada puede sufrir consecuencias tanto en vía administrativa como en la civil, si carece de las pertinentes medidas de seguridad:

- La responsabilidad contractual (art. 1101 CC y siguientes) y extracontractual por obligaciones que nacen de la culpa o negligencia (art. 1902 y 1089 CC), encuentran su justificación en el deber general de no dañar a terceros, adoptando las medidas de seguridad necesarias y actuando con la debida diligencia.

- No obstante, la Organización puede quedar exonerada de responder de aquellos daños que no hayan podido preverse, o cuando no quede demostrado el nexo de causalidad (art. 1.105 y 1.107 CC).

La Organización es responsable de los daños o perjuicios que el ciberataque haya podido causar a sus clientes. Por ello, es recomendable que, en el momento en que se sufra este tipo de ciberataques, se ponga en contacto tanto con los clientes que han podido verse afectados, para advertirles y que procedan a la modificación de sus credenciales, como con aquellos clientes que todavía no han sufrido, o no han notado, sus consecuencias, para prevenirles.

No debe olvidarse la legislación vigente en materia de Protección de Datos. El art. 32 RGPD señala respecto a la seguridad del tratamiento: *"Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo"*.

Se puede finalizar este apartado recordando que las organizaciones pueden llegar a ser responsables por su actuación u omisión, antes, durante y tras el ciberataque, ante la falta grave del deber de cuidado.

Concretando más, pueden serlo por el incumplimiento injustificado de la normativa vigente de Protección de Datos, ya sea antes del Ciberincidente (art. 32 RGPD, reproducido en el párrafo anterior) o después del mismo (art. 34 RGPD), que dispone: *"1. Cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento la comunicará al interesado sin dilación indebida"*, sin perjuicio de su comunicación a la autoridad de control, como puede ser en España la AEPD o, para el sector público, las agencias o autoridades autonómicas de protección de datos, de existir, según determina el art. 33 RGPD: *"En caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará a la autoridad de control competente de conformidad con el artículo 55 sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas"*.

NORMATIVA JURÍDICA RELACIONADA CON LA CIBERSEGURIDAD

Es evidente que, en función del sector de actividad de la Organización, o de sus potestades o competencias públicas, de tenerlas, podrá estar obligada por diferente normativa, además de, por ejemplo, el Esquema Nacional de Seguridad si pertenece al sector público, o le aporta soluciones o presta servicios.

A modo de ejemplo, podemos citar la reciente Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, en lo que respecta a sectores de alta criticidad (Anexo I) u otros sectores críticos (Anexo II) conocida como NIS2, que sustituye a la NIS1 traspuesta al ordenamiento jurídico español mediante el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, desarrollado mediante el Real Decreto 43/2021, de 26 de enero.

Por otro lado, la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas, obliga a los sectores estratégicos Nacionales relacionados en su Anexo, estando desarrollada mediante el Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas en España.

Otro ejemplo es la Ley 11/2022, de 28 de junio, General de Telecomunicaciones, que comprende, entre otros, la instalación y explotación de las redes de comunicaciones electrónicas, así como la prestación de los servicios de comunicaciones electrónicas, incluyendo aspectos como son el secreto de las comunicaciones (Art. 58), Protección de Datos de carácter personal (Art. 60), Cifrado (Art. 62), e Integridad y seguridad (Art. 63).

Y así podríamos ir enumerando normas jurídicas vinculadas con la Ciberseguridad y/o la Seguridad de la Información, en función del tipo de Organización.

Para facilitar la labor de los Oficiales de Cumplimiento en este ámbito de la Ciberseguridad, el Boletín Oficial del Estado (BOE), edita los que se han dado en llamar Códigos electrónicos, conteniendo un compendio temático y actualizado de normativa vigente, que además admite suscripción gratuita al servicio de avisos sobre actualizaciones. Los dos códigos más relevantes, en materia de Ciberseguridad, son los siguientes:

- **Código de Derecho de la Ciberseguridad:** Incluye normativa de Seguridad Nacional; Infraestructuras críticas; normativa de seguridad; Equipo de respuesta a incidentes de seguridad; telecomunicaciones y usuarios; Ciberdelincuencia, Protección de Datos; y relaciones con la Administración.

- **Ámbitos de la seguridad Nacional - Ciberseguridad:** Incluye normativa sobre Protección de Datos; ciberamenazas y seguridad en el Ciberespacio - cooperación en materia de seguridad; Infraestructuras Críticas en España; y uso eficiente de las Tecnologías de la Información.

RESUMEN FINAL

Como resumen, podemos llegar a afirmar que la Ciberseguridad ya no es una disciplina ajena al **cumplimiento normativo,** sino que, para muchas organizaciones, es un requisito específico de cumplimiento, **de forma directa,** y un facilitador de otras obligaciones normativas, **de forma indirecta.**

ISO 37002:2021 SISTEMAS DE GESTIÓN DE LA DENUNCIA DE IRREGULARIDADES “LA EVOLUCIÓN DE LOS CANALES DE DENUNCIAS”

Carlos Rozen
Socio de BDO en Argentina
Director de la Certificación Internacional en Ética y Compliance (AAEC – UCEMA)

En la actualidad, la ética y la integridad se han convertido en factores críticos de éxito para la sostenibilidad, y en algunos casos para la supervivencia, de las organizaciones. La implementación de pautas que fomenten una cultura del comportamiento virtuoso no solo es deseable, sino que se ha vuelto imperativa tanto a los ojos de los demás jugadores del mercado, como de los mismos reguladores.

El conjunto de elementos y herramientas que buscan prevenir comportamientos no deseados, detectarlos cuando estos ocurren y actuar en consecuencia se agrupan en programas de compliance, o, mejor aún, en sistemas de gestión de compliance.

Un elemento de gran importancia en este sentido es el canal de reporte o de denuncias, que permite identificar problemas relacionados con el comportamiento inapropiado, el fraude, la corrupción y otras formas de conducta contraria a los valores de una organización.

En este contexto, la norma ISO 37002 ha surgido como una guía esencial para ayudar a las organizaciones a establecer sistemas efectivos de gestión de denuncias. La ISO 37002 proporciona un marco concreto y sólido que permite establecer procesos y procedimientos robustos que promuevan una cultura de denuncia en los casos que corresponda, de manera tal de conseguir proteger a las partes interesadas con vinculación en cada caso, y garantizando la confidencialidad, imparcialidad y diligencia en la gestión de estos reportes. De esta forma ISO 37002 se constituye en una guía para que las organizaciones puedan establecer, implementar, mantener y mejorar en forma continua un sistema de gestión de denuncias.

LA IMPORTANCIA Y FORTALEZA DE IMPLEMENTAR SISTEMAS DE GESTIÓN

Las sobradas décadas de experiencia que el mundo tiene respecto de la utilización de sistemas de gestión integrados y certificables, a partir del ícono de “la ISO 9001”, nos clarifica que se trata de métodos probados que consiguen “motorizar” los programas o sistemas, de la especialidad que fueren.

Los sistemas de gestión utilizan elementos y herramientas comunes entre sí, que nos ayudan a comprender el diferencial entre escribir documentos, comunicarlos y exigir su cumplimiento, y hacer que realmente funcionen, es decir, que sean efectivos. Y cuando hablamos de efectivos nos referimos a la efectividad como un aspecto no solo perceptivo, sino que los mismos estándares relativos a estas normas de sistemas de gestión solicitan expresamente como requisito que sean medidos y mejorados en forma continua.

¿QUÉ ES LA “ESTRUCTURA DE ALTO NIVEL”? ¿CÓMO APROVECHARLA?

Desde la publicación de la norma ISO 9001 en su versión 2015, hemos venido hablando de un nuevo esquema diseñado por la Organización Internacional de Normalización (ISO) que implica que las normas de gestión bajo el estándar ISO respondan a un formato denominado “estructura de alto nivel” o mundialmente conocida con sus iniciales en inglés “HLS”, caracterizado por una serie de elementos comunes (apartados, secuencia, texto y terminología), lo que favorece notablemente la armonización entre los distintos sistemas de gestión.

De esta forma las organizaciones pueden adoptar ISO 37002 como guía independiente para su organización o, en el mejor de los casos, si ya tienen otros estándares implementados tales como ISO 37001 (Sistemas de Gestión Antisoborno), ISO 37301 (Sistemas de Gestión de Compliance), ISO 9001 (Sistemas de Gestión de Calidad), ISO 14001 (Sistemas de Gestión Ambientales), para citar solo algunos de ellos, podrán aprovechar una gran cantidad de elementos como los equipos de Auditoría Interna, las Revisiones por la Dirección, las políticas y procedimientos de documentos y registros, las capacitaciones, entre otros, permitiendo también planear las visitas de auditoría por parte del ente de certificación de manera conjunta e integrada.

Un aspecto notorio que formó parte de la discusión de la norma es que la presente guía podría ayudar a motorizar otros estándares (Ej.: si la organización tiene implementada ISO 14001, podría utilizar ISO 37002 para abordar los requisitos relacionados con la denuncia de irregularidades Medioambientales).

Es el punto 8 “Operación del Sistema de Gestión” el que presenta mayor diferencia entre norma y norma y el que le confiere realmente la particular identidad de cada una.

Otro aspecto de notoriedad es que ninguno de los puntos 1 al 10 utiliza la palabra mágica en este tipo de normas orientadas a compliance: “riesgos”. Sucede que el sistema de gestión que nos convoca, es un importante mitigador de riesgos de diversa naturaleza, estratégicamente diseñado para identificar, analizar, evaluar y responder a los riesgos específicos derivados de las denuncias.

¿DENUNCIAS?

La norma se refiere a “denuncia de irregularidades”, y así han sido extraídas estas palabras y traducidas en España (UNE-ISO) y otras países hispanoparlantes partir de su título “Whistleblowing Management System”. En lo personal pondré en tela de juicio si “denuncia” es la expresión más atinada para este tipo de acción humana a la que prefiero llamar “reporte” o como hace el legislador español en la Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción”, “informaciones” o “comunicaciones”.

Se trata de informar sobre sospechas de irregularidades o riesgo de estas, más que referirnos a un hecho estrictamente confirmado. Una de las definiciones más aceptadas de “denuncia” es “comunicar a una autoridad que se ha cometido un delito o que alguien es el autor de un delito”. Luego de haber hecho esta aclaración, tomaré reporte o denuncia de manera indistinta en el presente artículo.

¿IRREGULARIDADES?

El título de esta norma en inglés es **"Whistleblowing Management Systems".** Una traducción al español adecuada sería "Sistemas de Gestión de Denuncias". No obstante, el título que se le ha dado a la traducción oficial ISO-UNE es **“Sistemas de Gestión de la Denuncia de Irregularidades”**. La primer duda que me surgió con las normas en inglés y su traducción en español en la mano fue ¿por qué agregar la palabra irregularidad? Y ¿por qué irregularidad y no también fraude?

Cuando hablamos de **irregularidad** nos referimos a aquellas acciones, actos o comportamientos que se desvían o incumplen las normas, políticas, procedimientos establecidos en una organización, o bien, leyes o regulaciones que dicha organización debe cumplir. Estas acciones pueden ser o no intencionales, aunque generalmente no tienen el propósito directo de obtener beneficios personales o causar daño deliberado a la organización. Las irregularidades pueden manifestarse a través de violaciones de políticas definidas, incumplimientos de procedimientos establecidos, errores administrativos, negligencia en el cumplimiento de deberes, entre otras posibilidades.

Por su parte, el **fraude** implica un comportamiento intencional y engañoso realizado con el propósito de obtener beneficios personales o causar daño a otra persona o entidad, incluida una organización. Implica una conducta deliberada y maliciosa que tiene por objeto engañar, manipular o defraudar a otras personas para obtener beneficios financieros, bienes, servicios o ventajas indebidas. El fraude puede involucrar actividades como falsificación de documentos, robo de activos, malversación de fondos, manipulación de registros contables, soborno, o cualquier otra acción ilegal o antiética direccionada a obtener beneficios injustos.

Explicada esta distinción, propongo considerar que la norma ISO 37002 adopta el término "denuncia de irregularidades" para abarcar un espectro más amplio de conductas inapropiadas y promover una cultura de denuncia ética en las organizaciones, más allá de los casos específicos de fraude que, las personas más técnicas podrían diferenciar de las irregularidades.

GESTIONANDO LOS RIESGOS DE COMPLIANCE

La ISO 37002, al igual que otros sistemas de gestión relacionados con el Compliance tales como la ISO 37001 (Sistemas de Gestión Antisoborno) y la ISO 37301 (Sistemas de Gestión de Compliance) se apoya en la ISO 31000 (Sistemas de Gestión de Riesgos), concentra el foco en riesgos particulares de Compliance. Un Sistema de Gestión de Denuncias es un fuerte mecanismo de control a nivel de organización que funciona como mitigante de un amplio grupo de riesgos relacionados con todas las disciplinas de compliance que se definan dentro de su alcance.

¿UN MERO DISPOSITIVO?

La ISO 37002 pone de manifiesto la diferencia que existe entre una actividad de control y un sistema de gestión. No se trata de implementar solo un conjunto de canales que permitan recibir denuncias basados en un método y determinada tecnología. ISO 37002 implica establecer y llevar a cabo un conjunto de procesos y normas interrelacionadas que pretenden mitigar en forma eficaz un grupo de riesgos significativos relacionados con el comportamiento no deseado.

LA IMPORTANCIA DE LOS CANALES DE DENUNCIA

Encuestas y estudios realizados durante

la última década, sumados a la experiencia acumulada de muchas organizaciones demuestran el elevado nivel de efectividad de estos dispositivos para que salgan a la luz conductas indeseables. Lo que era hasta hace pocos años un dispositivo experimental algo temido y/o resistido por algunos directivos conservadores, hoy se ha perfilado como el mecanismo más virtuoso para identificar actos irregulares, antiéticos y/o fraudulentos.

Cada vez más organizaciones están considerando la posibilidad de introducir o mejorar políticas internas de denuncia de irregularidades, procedimientos, protocolos y dispositivos consecuentes, incluyendo la necesaria tecnología aplicada. En algunos casos responde a regulaciones (de hecho en España a partir de la antes citada Ley 2/2023 que desde el 13 de marzo de 2023 está en vigor para organizaciones con 249 trabajadores o más, y ayuntamientos con 10.000 o más habitantes) y en otros casos es implementado de manera voluntaria.

Anualmente el ACFE (Asociación de Examinadores de Fraudes Certificados) emite el "Reporte de las Naciones" con estadísticas muy interesantes referidas al fraude organizacional. Los resultados volcados en este informe revelan la relevancia de los dispositivos implementados para reportar irregularidades y fraudes. Veamos algunos resultados de la última versión del estudio emitido en 2022:

- Las organizaciones pierden en promedio un 5% de sus ventas por hechos de fraude.
- El 42% de los fraudes son detectados a través de denuncias.
- De estas denuncias más de la mitad son efectuadas por empleados de la organización, el 18% por parte de clientes, el 16% no se sabe (por ser anónimas) y el 10% por proveedores.
- Los canales de denuncia son un mecanismo 3 veces más poderoso que la labor de auditoría interna para detectar fraudes, con un costo decenas de veces menor.
- La duración promedio de un fraude en organizaciones con canales de denuncia es en promedio un 33% menor y de la mitad en pérdidas económicas.
- En los últimos 10 años se ha incrementado un 16% el uso de este tipo de dispositivos.
- El email sigue siendo el medio más utilizado, le siguen las aplicaciones web (que están ganando terreno) y luego las llamadas telefónicas (que están declinando en su uso).

¿QUÉ PRETENDE EN DEFINITIVA ISO 37002?

Hay quienes dicen que ISO de cualquier cosa arma un estándar. No es momento de entrar a valorar este tipo de opiniones, pero considerando la importancia práctica de los canales de denuncia, el intento por transformarlos en verdaderos sistemas de gestión merece ser considerado como un gran acierto, partiendo de datos como el de que esa pérdida promedio del 5% de las ventas por hechos de fraude, podría verse significativamente disminuida por causa de una herramienta que tiene un costo muy bajo, de tal modo que su migración hacia un enfoque más robusto y holístico podría reflejarse en ahorros muy significativos.

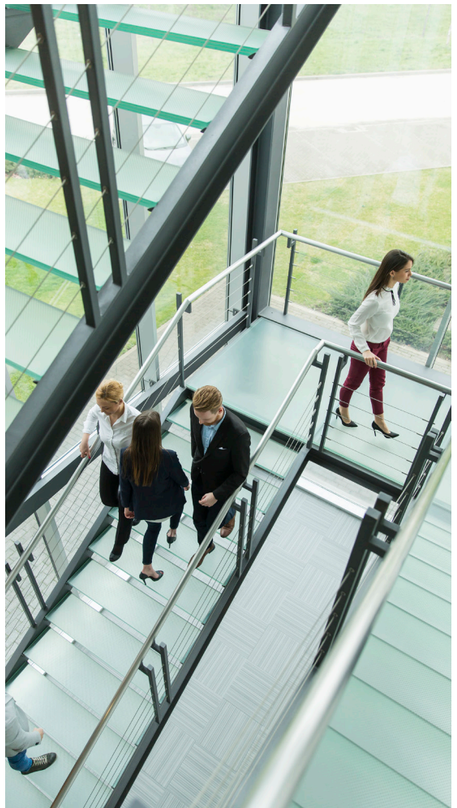
La ISO 37002 pretende, entre otras cuestiones:

- Alentar y facilitar el reporte de situaciones irregulares;
- Apoyar y proteger a quienes realizan estos reportes, y si fuera necesario, a otras partes interesadas involucradas;
- Otorgar certeza que las denuncias se reciban íntegramente y se traten de manera adecuada y oportuna;
- Fortalecer la cultura ética y el buen gobierno corporativo;
- Reducir los riesgos de irregularidades, actuando también como medida preventiva / disuasoria.

Si todo esto ocurriera, una organización podría esperar de la correcta implementación del sistema de denuncias, beneficios tales como:

- Identificar y abordar las irregularidades con la diligencia y agilidad que la situación merezca, teniendo en cuenta que detrás de una denuncia podrían existir riesgos elevados de que la organización pudiera ser sometida a la acción de la Justicia con impacto eventual en la reputación de la organización.
- Contribuir a prevenir o minimizar la pérdida de activos, y, en el mejor de los casos ayudar a la recuperación de éstos. Nótese que la recuperación de activos es una situación de difícil materialización en la mayoría de los fraudes investigados; sin embargo, las denuncias que incluyen pruebas al respecto pueden facilitar significativamente esa recuperación.
- Asegurar el cumplimiento de los códigos de comportamiento, las políticas, los procedimientos, las instrucciones operativas y las obligaciones legales y regulatorias de la organización;
- Atraer y retener personal comprometido con los valores y la cultura de la organización;
- Mostrar solidez a través de buenas prácticas de compliance hacia las partes interesadas, incluyendo los mercados, los reguladores, los propietarios, los clientes, proveedores, posibles inversores, entre otros.

Por otro lado, una adecuada implementación del sistema de denuncias, bien comunicada a las partes interesadas



(internas y externas a la organización), debería lograr:

- Demostrar el compromiso del liderazgo para prevenir y abordar las irregularidades;
- Alentar a las personas a que den a conocer los hechos irregulares que conozcan, en forma veloz, antes de que los problemas escalen y/o produzcan daños mayores;
- Reducir y prevenir las represalias contra los denunciantes de buena fe;
- Fomentar una cultura de apertura, transparencia, integridad y responsabilidad.

¿ES POSIBLE CERTIFICAR ESTA NORMA?

En la versión actual, se trata de un Estándar ISO del "tipo B" (directrices). Lo primero que los expertos suelen responder que, por lo tanto, no es una norma certificable. Sin embargo, numerosos entes de certificación suelen realizar un tipo de auditoría basada en métodos aceptados que les permiten concluir respecto de la adecuada implementación, funcionamiento y mejora continua del sistema de gestión en cuestión, y de esta manera emitir un certificado, aunque sin la participación de un ente de acreditación de nivel superior.

¿CUÁLES SON LOS PRINCIPIOS CLAVE DE LA NORMA?

El estándar se basa en determinados principios cuya comprensión nos ayuda a entender mejor muchos de sus apartados. Estos son:

Confianza: Se trata de un principio fundamental en la gestión de denuncias que implica crear un entorno en el que las personas que realizan reportes sientan seguridad y comodidad al informar sobre conductas inapropiadas o éticamente cuestionables. Es sabido que la confianza no es un atributo que se construye a través de una mera política. Resulta esencial que las organizaciones establezcan mecanismos claros y efectivos de comunicación y respuesta a las denuncias, garantizando la confidencialidad, el respeto y la protección de los denunciantes. Se necesitan muchos meses de buen funcionamiento en este sentido para desarrollar esta confianza.

Imparcialidad: Se refiere a la objetividad y justicia en la gestión de las denuncias. Es fundamental que las organizaciones traten todas las denuncias de manera equitativa, independientemente de quién sea el denunciante o el denunciado. La imparcialidad implica aplicar procedimientos y criterios uniformes y transparentes para investigar y evaluar las denuncias, evitando cualquier forma de discriminación o favoritismo.

Protección: El principio de protección que propone ISO 37002 se refiere a la salvaguarda de los denunciantes, pero no solo de estos, sino que también de otros involucrados en el proceso de reporte, que puedan sufrir algún tipo de problema derivado de su accionar. Las organizaciones deben tomar medidas para proteger a los denunciantes de posibles represalias, ya sea por parte de la persona o entidad denunciada o por otros miembros de la organización. Esto implica establecer políticas y procedimientos claros para garantizar la confidencialidad de la información proporcionada, así como brindar apoyo y asistencia a los denunciantes que puedan verse afectados negativamente como resultado de su denuncia. La protección no solo procede a pedido de quien teme por ello, sino que la organización debe comprender con una mirada amplia qué partes podrían sufrir consecuencias en cada hecho denunciado y actuar proactivamente en su protección.

¿ES UNA NORMA SOLO PARA UNAS POCAS ENTIDADES?

Por definición y análogamente a otras normas de este tipo, cualquier tipo de entidad puede implementar la norma. Es adaptable y su uso variará con el tamaño, naturaleza, complejidad y localización de las actividades del ente que desee implementarla.

Las pautas de la norma son genéricas y están destinadas a ser aplicables a todas las organizaciones, independientemente del tipo, tamaño, naturaleza de la actividad, y si en el sector público, privado, con o sin fines de lucro.

Tampoco la aplicación es restrictiva para aquellas organizaciones que ya tengan canales de denuncia en funcionamiento. El estándar puede ayudar a una organización tanto a mejorar sus herramientas y política y procedimientos de denuncia de irregularidades existentes, También puede ayudar a que una organización adapte su sistema de denuncias a nuevos requerimientos legales.

LOS GRANDES PASOS QUE PROPONE ISO 37002

Existen cuatro momentos considerados por ISO 37002 fundamentales en el proceso de denuncia de irregularidades. Pueden resultar algo obvios, aunque la norma pide tratar los mismos con mucho cuidado y dejando adecuadas evidencias de todo lo que va aconteciendo. Al seguir estos pasos de manera efectiva, las organizaciones pueden gestionar eficazmente las denuncias de irregularidades, promoviendo los beneficios mencionados en apartados anteriores.

- **Recibir reportes de irregularidades:** Este primer paso implica establecer un proceso claro y accesible para que los empleados, clientes u otras partes interesadas puedan presentar denuncias de irregularidades de manera confidencial y segura. Las organizaciones deben proporcionar canales de comunicación adecuados, como líneas directas, buzones de denuncias o plataformas en línea, para recibir estos reportes. Es fundamental que los denunciantes se sientan seguros al presentar sus denuncias y que se promueva una cultura de confianza y transparencia.
- **Evaluar los reportes de irregularidades:** Una vez que se reciben los reportes de irregularidades, es importante llevar a cabo una evaluación adecuada y objetiva de cada denuncia. Este paso implica revisar la información proporcionada, verificar su veracidad y determinar la gravedad y el alcance de la irregularidad reportada. Se pueden establecer criterios o pautas para clasificar y priorizar las denuncias en función de su importancia y riesgo potencial para la organización.
- **Abordar las denuncias de irregularidades:** Una vez evaluados los reportes, es crucial tomar medidas apropiadas para abordar las denuncias de irregularidades. Esto puede implicar la apertura de investigaciones internas, la asignación de responsabilidades y recursos para llevar a cabo la investigación y la implementación de medidas correctivas o preventivas necesarias. Es importante que el proceso de abordar las denuncias sea imparcial y justo, y que se garantice la confidencialidad tanto para los denunciantes como para las personas involucradas en la investigación.

- **Concluir acerca de los casos de denuncia de irregularidades:** En este último paso, se llega a una conclusión basada en los hallazgos de la investigación y se toman las medidas necesarias para resolver la irregularidad reportada. Puede implicar la aplicación de sanciones disciplinarias, mejoras en los controles internos o la implementación de políticas y procedimientos actualizados. Además, se debe comunicar el resultado de la investigación a los denunciantes, siempre respetando la confidencialidad y protección de las partes involucradas.

¿LA SEGURIDAD DE LA INFORMACIÓN?

Los sistemas de gestión de la denuncia de irregularidades inexorablemente manejan información que debe de ser tratada con las debidas medidas de seguridad.

Siempre intentando aprovechar la mencionada "estructura de alto nivel", no tengo mejor recomendación que recurrir a la familia de normas ISO 27000; además, por la robustez de estos estándares, nos ayudarán de manera muy precisa a interpretar y abordar mejor estos temas. ¿Qué es ISO 27000? Es un conjunto de estándares internacionales sobre la Seguridad de la Información. La familia ISO 27000 contiene un conjunto de buenas prácticas para el establecimiento, implementación, mantenimiento y mejora de Sistemas de Gestión de la Seguridad de la Información.

Existen al menos dos aristas relevantes que no podemos dejar de abordar: (a) Protección de datos personales, y (b) Confidencialidad. Sin embargo, no nos limitaremos a estos aspectos para constituir un sistema de gestión de denuncias.

¿UX / UI EN LOS SISTEMAS DE GESTIÓN DE DENUNCIAS?

Es muy usual en el plano de los desarrollos tecnológicos (y sin olvidar que los dispositivos para realizar denuncias utilizan la tecnología de manera creciente), hablar de: "UX = User Experience" (experiencia del usuario) y "UI = User Interface" (interfaz del usuario).

¿Qué significa esto? Resulta fundamental que los canales de reporte, por más robustos que se supongan, sean probados por los usuarios y en todos los niveles de la organización y se los escuche en cuanto a su experiencia general y de aspectos particulares. Muchas veces pueden ser de complejo acceso, uso, poco amigables, contenedores de errores, demoras, entre otros posibles problemas.

¿DE QUÉ SE TRATA LA FUNCIÓN DE GESTIÓN DE LAS DENUNCIAS?

Un aspecto saliente de la norma es que pone énfasis en los tiempos y prioridades de la función de Compliance para la debida gestión de los canales. El estándar dispone que se designe un responsable que lidere operativamente su buen funcionamiento con más un conjunto de recursos humanos y materiales que tengan relación con el dimensionamiento de actividades que merezca. La norma no pretende que exista necesariamente un departamento exclusivo para administrar el sistema de gestión de la denuncia de irregularidades. De hecho, la inmensa mayoría de las organizaciones que recibe denuncias ha tercerizado tanto la tecnología como la atención. Sería razonable suponer como alternativa que dependa de la función de Compliance.

EL TRIAGE

La norma aborda el concepto de "triage" (concepto extraído de la medicina que se refiere al establecimiento de un sistema de priorización para la atención de pacientes sobre la base del riesgo). De igual manera propone una evaluación del reporte inicial recibido, los efectos de la categorización, la adopción de medidas preliminares, la priorización y la asignación para su posterior manejo.

A los citados fines destaca que deberían considerarse factores tales como probabilidad e impacto de la irregularidad y/o delito (verificados o sospechados), el nivel jerárquico de las personas involucradas, o el tipo de tercero del cual se trate, la consideración del impacto reputacional, financiero, ambiental, en la salud de las personas u otros daños y perjuicios.

Aunque la norma no lo especifica, las buenas prácticas indican que en ninguna circunstancia el triage podrá ser empleado como un mecanismo para la no consideración de un caso denunciado.

La Mejora Continua

Si analizamos la estructura de la norma de manera holística, podremos encontrar en el último de los componentes comunes a todos estos estándares ISO, lo que llamamos "mejora continua". Se trata de un método para identificar puntos de mejora y remediar toda falla o debilidad en forma continuada colocando el sistema en un nivel superior de madurez día a día, mes a mes y año a año.

Los cuatro pasos clave en el proceso de mejora continua son los siguientes:

Planificar (Plan): En este paso, se identifican los objetivos de mejora y se establecen las estrategias y los planes de acción para alcanzarlos. Se recopila información relevante, se analizan los datos existentes y se realizan evaluaciones para comprender la situación actual y definir metas claras y medibles.

Hacer (Do): Aquí se implementan las acciones planificadas. Se ejecutan los planes de mejora, se realizan los cambios necesarios y se llevan a cabo las actividades previstas. Es importante documentar las acciones tomadas y recopilar datos sobre los resultados obtenidos.

Verificar (Check): En esta etapa se evalúa la efectividad de las acciones implementadas. Se comparan los resultados obtenidos con los objetivos establecidos y se analiza si se han logrado las mejoras esperadas. Se utilizan técnicas de medición y monitoreo para recopilar y analizar datos relevantes y evaluar el impacto de los cambios realizados.

Actuar (Act): Por último, se toman decisiones basadas en los resultados y las evaluaciones realizadas. Si los resultados son satisfactorios, se estandarizan y se incorporan las mejoras como prácticas habituales. Si se identifican deficiencias o áreas de mejora adicionales, se desarrollan planes de acción para abordarlas. El ciclo continúa con la implementación de las acciones correctivas o preventivas necesarias.

EL CONTENIDO DE LA ISO 37002

Si bien el presente artículo está lejos de ser una norma comentada, a continuación, se detalla el contenido de la norma para tener una visión resumida.

A su vez se coloca cada capítulo dentro de las cuatro etapas de la mencionada "mejora continua".

PLANIFICAR	HACER	VERIFICAR	ACTUAR
4.1 Comprensión de la organización y su contexto. 4.2 Comprensión de las necesidades y expectativas de las partes interesadas. 4.3 Determinación del alcance. 4.4 Sistema de Gestión de la denuncia de irregularidades. 5.1 Liderazgo y compromiso. 5.2 Política de denuncia de irregularidades; 5.3 Roles, responsabilidades y autoridades. 6. Planificación; 6.1 Acciones para abordar riesgos y oportunidades. 6.2 Objetivos del sistema de gestión de la denuncia de irregularidades.	7. Apoyo; 7.1 Recursos; 7.2 Competencia. 7.3 Toma de conciencia y formación. 7.4 Comunicación. 7.5 Información documentada (creación, actualización, control). 7.5.4 Protección de datos. 7.5.5 Confidencialidad. 8. Operación del sistema. 8.1 Planificación y control operacional. 8.2 Recepción de denuncias. 8.3 Evaluación de denuncias. 8.4 Tratamiento de denuncias. 8.5 Conclusión de casos de denuncia.	9. Evaluación del desempeño; 9.1 Seguimiento, medición, análisis y evaluación. 9.2 Auditoria interna. 9.3 Revisión por la dirección. 9.4 Revisión de la función de Cumpl. Antisoborno.	10. Mejora. 10.1 Mejora continua. 10.2 No conformidades y acciones correctivas.

¿CÓMO DEBERÍA ARTICULARSE EL PROGRAMA DE AUDITORÍA INTERNA DE UN SISTEMA DE GESTIÓN DE DENUNCIAS?

La organización debería planificar, establecer, implementar y mantener un programa de auditoría, incluyendo la definición de aspectos relevantes tales como la frecuencia en la ejecución de los trabajos de auditoría, los métodos a utilizar, las responsabilidades tanto de la auditoría como de otras partes interesadas (Ejemplo: de quienes deben recibir a los auditores internos), los requisitos de planificación de las auditorías y los informes a presentar.

Al establecer los programas de auditoría interna, la organización debería considerar la importancia de los procesos que serán objeto de la auditoría y los resultados de auditorías anteriores.

La entidad debería definir los objetivos, criterios y alcance de la auditoría para cada auditoría. Seleccionar auditores y realizar auditorías para garantizar la objetividad y la imparcialidad del proceso de auditoría. Asegurarse que los resultados de las auditorías sean informados a la dirección para que adopte las adecuadas decisiones. Tener certeza de que los resultados de la auditoría se consideren y se actúe según corresponda. Disponibilizar la información documentada como evidencia de la implementación del programa de auditoría interna y de los resultados obtenidos de la ejecución de la auditoría.

CONCLUSIONES

Hemos explorado en este artículo algunos aspectos distintivo de los sistemas de la gestión de denuncias según lo propuesto por la norma ISO 37002. Asimismo hemos destacado cómo esta norma puede fortalecer la cultura organizacional, fomentar la confianza y la transparencia, y mejorar el cumplimiento de normas éticas y legales, como así también resaltado los beneficios que las organizaciones pueden obtener al implementar este estándar.

El futuro de la gestión de denuncias éticas es promisorio por su elevado poder de revelar la existencia y modalidad con la cual ocurren situaciones no deseadas, y considerando las tendencias emergentes, requerimientos legales y regulatorios, encuestas analizadas y los cambios en la cultura ética de las organizaciones.

Implementar la norma ISO 37002 en su organización, promoviendo una cultura de denuncias de buena fe y contribuir al desarrollo de entornos empresariales más éticos y responsables es esencial.

Si llegaste al final del artículo puedes descargarte mi libro digital sobre ISO 37002 de manera gratuita haciendo click aquí

CORRUPCIÓN, DENUNCIAS INTERNAS Y ALGUNAS REFLEXIONES EN TORNO AL SISTEMA INTERNO DE INFORMACIÓN CREADO POR LA LEY 2/2023

DE 20 DE FEBRERO, REGULADORA DE LA PROTECCIÓN DE LAS PERSONAS QUE INFORMEN SOBRE INFRACCIONES NORMATIVAS Y DE LUCHA CONTRA LA CORRUPCIÓN.

Alejandro Cabaleiro
Fiscal de la Fiscalía especial contra la corrupción y la criminalidad organizada

Aunque la corrupción no existe como tipo delictivo autónomo, no cabe duda de la importancia del concepto en nuestros días. Quizá pueda sorprender, no obstante, que no fue hasta hace relativamente poco tiempo cuando se comenzó a mostrar preocupación legislativa por su regulación. Así, desde la inicial Convención de la Naciones Unidas contra la Corrupción de 31 de octubre de 2003, es mucho lo que se ha avanzado.

Ello podría resultar extraño, pues parece evidente que desde el origen de las civilizaciones muchas de las conductas consideradas como corrupción, han sido perseguidas y sancionadas. Se trata de un fenómeno a nivel global e intergeneracional que, desde la normativización en el ámbito internacional asociado a conductas delictivas graves y muy perjudiciales para la sociedad, ha ido calando

en un espacio normativo que ya estaba interiorizado en el general de las sociedades.

Mucho se ha escrito y hablado con relación al moderno derecho penal y a la ampliación de su campo de protección, con la aparición de los delitos de tercera generación vinculados al campo tradicional del derecho administrativo sancionador. Las difíciles fronteras entre uno y otro, los tradicionales problemas de delimitación tanto formal como material, se reproducen en el ámbito de la corrupción, su consideración y entendimiento. Todas las sociedades tienen una noción más o menos nítida de las conductas reprochables, socialmente aceptadas y permitidas, tanto desde una perspectiva moral como jurídica no siempre coincidentes.

Si entendemos la noción de función pública como servicio público de acuerdo con unas pautas objetivas, presidido por los principios constitucionales de igualdad, mérito y capacidad, podría decirse que corrupción debería ser todo aquello que infringiese tales presupuestos, tanto desde un punto de vista interno como externo. Sin embargo, tal visión conlleva el inevitable inconveniente del sesgo propio de las personas que participan en tales funciones.

La noción de sesgo, de carácter psicológico, no puede ser desatendida. Cada persona tiene una forma diferente de enfrentarse, o de visualizar lo correcto y lo incorrecto, desde sus propias vivencias (educación, familia, experiencias previas etc.) marcan las pautas personales. Ello tiene una notable importancia en un país, como el nuestro, en el que las fronteras entre "corruptelas" / "corrupción administrativa" y "corrupción penal" no siempre son claras, o al menos, no siempre son entendidas desde la misma perspectiva por las diferentes personas llamadas a intervenir desde diferentes ámbitos en un expediente.

Graduación, desde las conductas socialmente aceptadas hasta las delictivas: Desde una perspectiva moral, podríamos partir del máximo por todos conocidos de que "la mujer del César no sólo tiene que ser honesta, sino también parecerlo", pues tal expresión encuentra un acercamiento, vulgar pero interesante, a la materia y, seamos claros, es ampliamente rechazado por muchas personas, pues nos llevaría a aceptar que corrupción no es solo la representada por grandes hechos delictivos, sino que también existe en conductas mucho más nimias a los ojos de muchas

personas. La teoría general del derecho recurre a un concepto más elaborado. Así, se alude a las conductas socialmente aceptadas, aplicadas a regalos de cortesía para declarar atípicas las mismas. Regalos, favores o dádivas que se pueden ofrecer a un empresario o a un funcionario público y que, aún aceptadas, se considera que no revisten carácter delictivo.

Siendo el anterior el primer escalón de la corrupción, el mismo asciende con conductas difusas que en algunos casos han llegado a aceptarse a pesar de su no menor coste económico. Así por ejemplo se encuentra dentro de ese campo oscuro la invitación al palco de un estadio de futbol, a pesar del alto valor económico que puede suponer.

Siguiendo con la graduación, nos encontramos la corrupción prevista en las normas de derecho privado (civil), nueva muestra de conductas que pese a poder ser definidas dentro del concepto general no encuentran sanción penal.

Finalmente, como eslabón más alto, nos encontramos con la definición de corrupción a efectos penales, o sancionadores[1].

¿Cómo es posible que en el estado actual del desarrollo humano pueda seguir tal graduación de ámbitos? ¿Cómo es posible que no se haya podido definir la corrupción como tipo delictivo autónomo? Responder a estas preguntas no es el objeto de este artículo, pero aquí quedan al objeto de que puedan ser ob-

[1]El CGPJ especifica en su página web (www.poderjudicial.es/cgpj/Temas/Transparencia/ch.Repositorio- de-datos-sobre-procesos-por-corrupción/Informacion--general/) que **"Se consideran delitos relacionados con la corrupción a los efectos de este repositorio":**

- Negociaciones y actividades prohibidas a los funcionarios públicos y de los abusos en el ejercicio de su función Arts. 439, 441, 442 y 443 CP
- Malversación. Arts. 432, 433, 434 y 435 CP
- Cohecho. Arts. 419, 420, 421 y 422 CP
- Prevaricación de funcionarios públicos. Arts. 404, 405 y 408 CP
- Ordenación del territorio, urbanismo y patrimonio histórico. Arts. 320 y 322 CP
- Infidelidad en la custodia de documentos y violación de secretos. Arts. 413, 414, 415, 416, 417 y 418 CP
- Tráfico de influencias. Arts. 428, 429 y 430 CP
- Fraudes y exacciones ilegales. Arts. 436, 437 y 438 CP"

jeto de reflexión por parte del lector.

Necesariamente he de dejar al margen las cuestiones relativas a la posible corrupción de las conductas socialmente aceptadas y a corrupción en asuntos civiles, como son por ejemplo los casos de "puertas giratorias" pues, por más que desde la perspectiva moral subjetiva puedan ser definidas como corrupción, lo cierto es que en nuestro sistema no son ilegales, ni pueden dar lugar al inicio de una investigación que, de hacerlo, con casi toda probabilidad sería declarada prospectiva.

Precisamente esto nos ha de llevar a plantearnos, **cuáles son los requisitos básicos esenciales que permiten iniciar una investigación sin riesgo a ser declarada prospectiva.** Una cuestión de primer orden sobre la que merece la pena realizar alguna consideración, pues precisamente la primera actuación de una causa judicial resulta trascendental a la hora de valorar su idoneidad.

Pues bien, lo primero que puede llamarnos la atención es que, como tal "investigación prospectiva", no es una figura que se encuentre regulada en ninguna norma positiva. Ni la ley orgánica del poder judicial, ni la ley de enjuiciamiento criminal aluden a ella. Desde un punto de vista estrictamente etimológico, prospectivo es un adjetivo que se define como "que hace referencia a un tiempo futuro", a partir de tal concepto, y según en el campo en el que nos movamos o sobre el que lo apliquemos, implica cosas diferentes, pero siempre marcadas por la esencia del "análisis futuro". Una investigación será prospectiva cuando lejos de perseguir un hecho delictivo concreto, tenga por exclusiva finalidad indagar la conducta o actividad de una o varias personas que se presumen peligrosas o potenciales delincuentes atendidos sus antecedentes o su forma de vida, actual o pasada (vid. SSTS 795/2016, de 25 de octubre; 144/2015, de 13 de octubre; 288/2013, de 22 de marzo; 174/2001, de 26 de julio). En palabras de la STC 184/2003, de 23 de octubre, se consideran prospectivas aquellas investigaciones que se sustenten «en meras hipótesis o en la pura y simple sospecha», es decir, que no cuenten con un mínimo fundamento objetivo y material susceptible de eventual verificación.

Es decir, una investigación será prospectiva cuando no exista prueba ni indicio alguno delictivo, de forma que se inicie la investigación a los efectos, no de investigar un hecho delictivo conocido a priori, sino que para averiguar si el mismo existe, sin más apoyo externo que, en el mejor de los casos, la intuición o la exigencia moral. Por poner el caso, la mera existencia de "una puerta giratoria" no es indicio alguno, e iniciar una investigación por el convencimiento moral de que tal conducta obedece a algún pacto o favor, previo o posterior, sería prospectivo. Cuestión diferente es recibir una denuncia (aunque fuese anónima) en que se afirmarse que tal autoridad pública mantuvo una reunión con un promotor inmobiliario y acordaron que, si la autoridad conseguía recalificar unos terrenos, posteriormente, cuando dejase su puesto público, sería contratada como asesor o nombrado miembro del consejo de administración. Tal supuesto, es igualmente "una puerta giratoria" más la existencia del indicio que constituye la denuncia inicial, permite iniciar la investigación.

Puede considerarse, por qué no, que **el carácter prospectivo en el ámbito del derecho penal constituye una injustificada limitación en la lucha contra la corrupción,** más ello sólo podrá ser argumentado en ámbitos académicos o teóricos; pues tanto la doctrina penalista como la jurisprudencia mantienen una postura ya consolidada que enlaza la prohibición del carácter prospectivo en las investigaciones con el derecho fundamental a la presunción de inocencia.

Esta postura garantista supone de facto que la lucha contra la corrupción, entendida como globalidad, parta, desde su origen, con una limitación procesal no menor, aunque en algunos ámbitos, especialmente vinculados a la corrupción económica (blanqueo de capitales y delitos tributarios esencialmente) **existe, como respuesta a esa limitación, la solución administrativa idónea que permite al amparo de la actividad de supervisión administrativa realizar inspecciones o investigaciones sin necesidad de que existan previos indicios infractores.** Así, cuando la AEAT, inicia un plan anual de inspección sobre ciertas actividades o profesiones liberales, lo hace al amparo de la supervisión en la gestión de los tributos y si como consecuencia de ello se aprecia la existencia de un delito fiscal, debería deducir el tanto de culpa a la jurisdicción penal sin que ello implique inicio prospectivo.

Sin embargo, en otros muchos ámbitos relacionados con la corrupción, no existe tal actividad de supervisión administrativa, con lo cual los inicios en las investigaciones pueden verse más comprometidos. Es precisamente en ese campo, donde cobra especial relevancia la idea de protección al denunciante, a la que el derecho procesal penal tradicional, venía dando respuesta (y sigue) a través de la figura del testigo protegido.

Leyendo la exposición de motivos de la Ley Orgánica 19/1994, de 23 diciembre, que regula la Protección a Testigos y Peritos en causas criminales, como los considerandos de la Directiva 2019/1937 del Parlamento Europeo y del Consejo, de 23 de octubre, como la exposición de motivos de la reciente Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción, se advierte que la justificación subyacentes a tales normas es la misma, a saber, tratar de salvar las reticencias de los ciudadanos a colaborar con las autoridades ante el temor de sufrir represalias.

Una vez comprobado que **el deber general de denunciar que tiene toda persona que presencia la perpetración de un delito** (ex artículo 259 de la Ley de Enjuiciamiento Criminal, concretado más taxativamente en el artículo 262 de la misma norma cuando se trate de personas que "por razón de sus cargos, profesionales u oficios tuvieren noticia de algún delito público, salvando las expresas exclusiones que al respecto se establecen para determinadas personas en los artículos 260 y 261), **no ha resultado efectivo, básicamente por el temor a represalias,** las normas citadas (ley de protección de testigos, Directiva y Ley de transposición) tratan de dar una solución práctica al problema, a través del diseño de un sistema que aleje el riesgo o temor a esas temidas represalias, intentando, con ocasión de la invocación de principios éticos y de gobernanza, implementar un sistema que cree o establezca la idea o sentimiento general en la sociedad de que, se deben denunciar aquellas conductas que revistan caracteres de delito o sanción administrativa, al tiempo que se garantiza que ello no va a implicar repercusiones en la vida del denunciante, ni de sus familiares, allegados, colaboradores o empresas.

Un estado de social y democrático de derecho no puede conformarse con la obligación formal de denuncia, al igual que no puede pretender hacer del denunciante un héroe civil, que expone su vida cotidiana, su tranquilidad personal, familiar y económica, sin ningún reparo. Vivir en sociedad implica deberes, pero también implica derechos, y una sociedad adulta no puede exigir los primeros y desatender los segundos. En tal sentido, podría decirse que el clima, o sensación generalizada existente, era precisamente ese. Toda persona que, presenciase un delito, o tuviese conocimiento de prácticas irregulares, tanto si provenían del sector público, como -y con más peso- si venían del sector privado, se exponía (y expone) al dilema de cómo actuar.

Sin entrar en consideraciones de tipo jurídico, ¿puede realmente reprochársele a una persona que, ante la situación descrita, decida "mirar para otro lado" antes de proceder a poner los hechos en conocimiento de las autoridades si la perspectiva es de desamparo ante las posibles represalias?, con el agravante de que, en la mayoría de los casos, tales represalias no serán directas, sino que se enmascararán como decisiones de tipo organizativo, económico o discrecional en muchos casos totalmente legales y previstas por la ley. **La Ley Orgánica de Protección de Testigos** no es sólo que no resolviese el problema, es que ni tan siquiera se planteaba al mismo. La idea o espíritu de tal norma, tiende a una protección *ad intra* del procedimiento, descontextualizado del día a día del denunciante. Se pretende garantizar el anonimato del denunciante durante el proceso penal, de forma que se pueda instruir un procedimiento recabando información de este al tiempo que la persona investigada desconozca la concreta fuente de la información. Ello hace que la ley exija una decisión judicial que declare tal protección tras analizar las concretas circunstancias, de conformidad con lo que establecen sus artículos primero[2] y segundo[3]. Determinada su idoneidad, la propia ley no establece un marco concreto que nos diga en qué ha de consistir la protección, delegando en el juez las medidas idóneas en cada caso, que pueden llegar "en casos excepcionales" a otorgársele una nueva identidad y medios económicos para cambiar su residencia o lugar de trabajo, de conformidad con el párrafo segundo del artículo tercero[4].

Lógicamente, en el ámbito del derecho procesal penal de un Estado de Derecho, tales medidas han de resultar igualmente compatibles con el derecho de defensa y ello, sobre la primacía de este último, manifestada en el derecho a conocer, llegado el momento procesal oportuno la identidad del testigo protegido. Al respecto, la ley dice en el apartado tercero de su artículo cuarto que: "Sin perjuicio de lo anterior, si cualquiera de las partes solicitase motivadamente en su escrito de calificación provisional, acusación o defensa, el conocimiento de la identidad de los testigos o peritos propuestos, cuya declaración o informe sea estimado pertinente, el Juez o Tribunal que haya de entender la causa, en el mismo auto en el que declare la pertinencia de la prueba propuesta, deberá facilitar el nombre y los apellidos de los testigos y peritos, respetando las restantes garantías reconocidas a los mismos en esta ley" de tal forma que la clave se halla en la necesidad de que la petición sea motivada y la posterior decisión del Tribunal al respecto y que, desde la perspectiva práctica general, ha sido tratado en múltiples resoluciones, así la jurisprudencia del Tribunal Supremo sobre esta materia, constituida básicamente por la STS 38/2019, de 15 enero, que condensa la contenida en otras anteriores, y que ha sido reproducida posteriormente, entre otras, en SSTS 422/2020, de 23 de julio; 580/2021, de 1 de julio; y la 155/2022, de 22 de febrero. Como recoge la Sentencia del Tribunal Supremo nº 575/2022 de 9 de junio esta postura jurisprudencial se conforma "a partir de las pautas que progresivamente han ido asentando el TEDH (especialmente en las SSTEDH recaídas en los casos Kostovski, de 20 de noviembre de 1989 ; Windisch, de 27 de septiembre de 1990; LUDI, de 15 de junio de 1992; Doorson, de 26 de marzo de 1996; Van Mechelen, de 23 de abril de 1997; Wisser, de 14 de febrero de 2002; Birutis, 28 de marzo de 2002; Taal, de 22 de noviembre de 2005; Al-Khawaja y Tahery, de 15 de diciembre de 2011; Hümmer, de 19 de julio de 2012 ; Gani, de 19 de febrero de 2013) y el Tribunal Constitucional (esencialmente a partir de las SSTC 64/1994, de 28 de febrero (EDJ 1994/1761) y 75/2013, de 8 de abril). Y proyectada desde la perspectiva del derecho a un juicio *público con todas las garantías consagrado en el artículo 24.2 CE, que a su vez es analizado desde una triple vertiente de exigencias: publicidad, contradicción e igualdad de armas".*

Siendo la Jurisprudencia conocida, **la cuestión práctica que toda persona se planteaba a la hora de proceder o no a denunciar, es que no tenía seguridad de que su identidad, finalmente no fuera desvelada al denunciado.** Como se expone en la Sentencia nº 12/2022, del 6 de octubre, de la Sección Primera de la Sala de lo Penal de la Audiencia Nacional, en su fundamento de derecho segundo, punto séptimo: "Donde se produce la discrepancia es en la forma de aplicar la doctrina jurisprudencial a este caso y en el cumplimiento de los requisitos que debe reunir la declaración del testigo protegido para su eficacia. En definitiva, de acuerdo con la jurisprudencia del Tribunal Europeo de Derechos Humanos, del Tribunal Constitucional y del Tribunal Supremo, para poder erigirse en prueba de cargo, la declaración del testigo protegido debe reunir tres concretos requisitos. El primero de ellos que la protección haya sido acordada por el órgano judicial en una decisión motivada en la que se hayan ponderado razonablemente los intereses en conflicto; el segundo, que los déficits de defensa que genera el anonimato hayan sido compensados con medidas alternativas que permitan al acusado evaluar y, en su caso, combatir la fiabilidad y credibilidad del testigo y de su testimonio; y el tercero, que la declaración del testigo protegido concurra acompañado de otros elementos probatorios, de manera que no podrá, por sí sola o con un peso probatorio decisivo, enervar la presunción de inocencia. Para el recurrente estos requisitos, pese a lo que se indica en la sentencia recurrida, no se cumplen, mientras que para el ministerio fiscal se cumplen y solicita en su escrito de oposición al recurso la confirmación de la sentencia".

[2] *1. Las medidas de protección previstas en esta ley son aplicables a quienes en calidad de testigos o peritos intervengan en procesos penales. 2. Para que sean de aplicación las disposiciones de la presente ley será necesario que la autoridad judicial aprecie racionalmente un peligro grave para la persona, libertad o bienes de quien pretenda ampararse en ella, su cónyuge o persona a quien se halle ligado por análoga relación de afectividad o sus ascendientes, descendientes o hermanos.*

[3] *Apreciada la circunstancia prevista en el artículo anterior, el Juez instructor acordará motivadamente, de oficio o a instancia de parte, cuando lo estime necesario en atención al grado de riesgo o peligro, las medidas necesarias para preservar la identidad de los testigos y peritos, su domicilio, profesión y lugar de trabajo, sin perjuicio de la acción de contradicción que asiste a la defensa del procesado, pudiendo adoptar las siguientes decisiones: a) Que no consten en las diligencias que se practiquen su nombre, apellidos, domicilio, lugar de trabajo y profesión, ni cualquier otro dato que pudiera servir para la identificación de los mismos, pudiéndose utilizar para ésta un número o cualquier otra clave. b) Que comparezcan para la práctica de cualquier diligencia utilizando cualquier procedimiento que imposibilite su identificación visual normal. c) Que se fije como domicilio, a efectos de citaciones y notificaciones, la sede del órgano judicial interviniente, el cual las hará llegar reservadamente a su destinatario.*

[4] *2. A instancia del Ministerio Fiscal y para todo el proceso, o si, una vez finalizado éste, se mantuviera la circunstancia de peligro grave prevista en el art. 1,2 de esta ley, se brindará a los testigos y peritos, en su caso, protección policial. En casos excepcionales podrán facilitárseles documentos de una nueva identidad y medios económicos para cambiar su residencia o lugar de trabajo. Los testigos y peritos podrán solicitar ser conducidos a las dependencias judiciales, al lugar donde hubiere de practicarse alguna diligencia o a su domicilio en vehículos oficiales y durante el tiempo que permanezcan en dichas dependencias se les facilitará un local reservado para su exclusivo uso, convenientemente custodiado.*

La conclusión es que **el denunciante no podía prever ex ante si finalmente su identidad sería revelada,** o no. Ningún operador jurídico (policía, fiscal o juez de instrucción) puede garantizarle tal hecho, pues lo única certeza es que una vez la causa llegue al Tribunal encargado del enjuiciamiento, será éste el que decida si desvelar o no la identidad del denunciante.

Bajo la esfera de la reciente ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción, la cuestión que nos planteamos es si la misma ha modificado el sistema.

Pues bien, respecto al ámbito material de aplicación, la ley, siguiendo a la Directiva[5], se limita a señalar en el apartado segundo de su artículo segundo que *"Esta protección no excluirá la aplicación de las normas relativas al proceso penal, incluyendo las diligencias de investigación"*, sin que la exposición de motivos aclare nada más, por lo que se desprende que existe un régimen de compatibilidad. La misma, resulta lógica en cuanto a la evitación de represalias y medidas destinadas a ello, no en el resto, en la medida que la ley de protección de testigos no se modifica.

Así las cosas, cuando un denunciante efectúe la denuncia a través de los mecanismos que prevé la ley, si los mismos son indiciariamente constitutivos de infracción penal, el denunciante quedará bajo el amparo de protección tanto de la nueva ley como de la de protección de testigo, claro está, en función de lo dispuesto en las mismas, ya que hay cuestiones, como la relativa al anonimato, en los que las disposiciones a aplicar serán las previstas en la normativa procesal y, en lo que no resulta incompatible con esta, lo dispuesto en la nueva ley. Es decir, un denunciante, a efectos de la entidad para la que trabaja, seguirá siempre gozando de la protección de la nueva ley, incluso respecto de la obligación de no revelar sus datos, pero ello no impedirá que, a efectos del proceso penal, la persona o personas denunciadas, puedan llegar a conocer su identidad de conformidad con lo que dispone la ley de protección de testigos.

Tal solapamiento de normativas, no solo se produce con relación a la protección del denunciante, también afecta al momento en que los hechos objeto de denuncia deban de ser conocidos por el Ministerio Fiscal.

Tanto si se recurre al "cauce preferente" del sistema interno, como si se hace a través del canal externo de información de la autoridad Independiente de protección del Denunciante, A.A.I., la ley prevé una remisión de actuaciones al Ministerio Fiscal o a la Fiscalía Europea, con carácter inmediato cuando los hechos pudieran ser indiciariamente constitutivos de delito y, en el segundo caso, afecten a los intereses financieros de la Unión Europea. Como cláusula de cierre, dentro de la actuación de la A.A.I. se prevé, como forma de terminación de las actuaciones, la "remisión al Ministerio Fiscal si, pese a no apreciar inicialmente indicios de que los hechos pudieran revestir el carácter de delito, así resultase del curso de la instrucción. Si el delito afectase a los intereses financieros de la Unión Europea, se remitirá a la Fiscalía Europea".

El Sistema Interno de información, previsto en la ley como el cauce preferente para denunciar, aunque dejando a criterio del denunciante la decisión de utilizarlo o no, en función de las consideraciones que el mismo pueda tener sobre el grado de seguridad que en cuanto a la confidencialidad de sus datos y protección le trasmita el sistema, en las cuales no vamos a detenernos.

Si merece la pena dejar planteadas algunas cuestiones con relación a las llamadas de investigaciones internas, cuya tramitación, deberá de encontrarse fundamentada en los principios de defensa y no auto incriminación.

La cuestión anterior no es baladí, seguramente sea la cuestión más crítica de la nueva regulación. En este punto, conviene señalar la especial importancia que conlleva que la información sea sobre hechos indiciariamente pudieran ser constitutivos de delito, y ello a efectos de alertar de que la aplicación práctica del sistema no debiera revertir el orden natural del proceso. "Indicio", conforme el Diccionario de la Real Academia de la Lengua Española es "1. Fenómeno que permite conocer o inferir la existencia de otro no percibido", "2. Cantidad pequeñísima de algo, que no acaba de manifestarse como mesurable o significativa" y que, trasladado al ámbito del proceso penal implica "indicios de criminalidad" entendidos como aquellos hechos que, sin constituir prueba directa sobre los mismos, aportan datos constatables con prueba directa de los que pueden inferirse la existencia de un delito.

La importancia del precepto cobra especial relevancia en aquellos supuestos en los que la información verse sobre hechos susceptibles de ser considerados tanto delito como infracción administrativa grave o muy grave, pues existen otros en los que no existirá posibilidad de duda alguna. Así, si la información consiste en que otro empleado ha accedido a la taquilla de un compañero violentando el candado, no cabe duda de que se tratará de un posible delito de hurto o robo, y deberá ser inmediatamente remitida la información a la Fiscalía sin iniciar proceso alguno de investigación. Por el contrario, en otros casos, como por ejemplo, una información en que el empleado traslada su opinión o creencia de que la contabilidad de la empresa es llevada de manera contraria a la normativa contable, no será fácil determinar inicialmente si la información debe ser considerada como presuntamente constitutiva de delito contable o infracción administrativa grave o muy grave, debiendo de analizarse por el responsable del sistema interno de información la relevancia indiciaria y el contenido de la información. Así, mientras que en casos de información general sobre malas prácticas contables será imposible determinar si existe presuntamente un delito o no y lo procedente será abrir una investigación interna, en otros, donde se acompañen pruebas concretas del falseamiento de datos contables, indiciarios de una conducta presuntamente delictiva, si procederá dar traslado al Ministerio fiscal.

Entiendo que, la correcta interpretación que debe de dársele a esta remisión al Ministerio Fiscal es la de una visión amplía, de forma que el responsable del sistema ponga los hechos en conocimiento de la Fiscalía desde el primer momento y, si ésta, rechaza la relevancia penal de la información, pueda entrar en juego -en su caso- la actividad de investigación interna. Tal interpretación, amén de ser la seguida en otras normativas, es la que resulta más garantista para todos los implicados o afectados por los hechos por cuanto la fiscalía deberá de incoar diligencias de investigación de

[5] Artículo 3.3 "La presente Directiva no afectará a la aplicación del Derecho de la Unión o nacional relativo a: a) la protección de información clasificada; b) la protección del secreto profesional de los médicos y abogados; c) el secreto de las deliberaciones judiciales; d) las normas de enjuiciamiento criminal". Y, en su considerando (28) establece que *"Si bien la presente Directiva debe de establecer, en determinadas condiciones, una exención limitada de responsabilidad, incluida la responsabilidad penal, en caso de violación de la confidencialidad, ello no debe afectar a las normas nacionales relativas al proceso penal, especialmente las destinadas a proteger la integridad de las investigaciones y procedimientos o los derechos de defensa de las personas afectadas"*.

conformidad con su Estatuto Orgánico y actual Circular de la Fiscalía General del Estado 2/2022. Por una parte, es la más garantista para el denunciado, en caso de encontrarse identificado, pues la circular establece que sin perjuicio de su condición extraprocesal (vid. SSTS 1394/2009, de 25 de enero; 228/2013, de 22 de marzo; 980/2016, de 11 de enero de 2017), las diligencias de investigación del Ministerio Fiscal se caracterizan por su naturaleza penal. Su objeto y efectos no permiten alcanzar otra conclusión. Esta conceptualización justifica la directa aplicación de las garantías reconocidas por el art. 24 CE y, en particular, de los derechos de defensa, asistencia letrada, información de los hechos imputados, a no declarar contra sí mismo y a no confesarse culpable, a la presunción de inocencia y, en definitiva, a un proceso público con todas las garantías; igualmente es la más aconsejable para la propia entidad, pues con ello evitará verse en la posible complicada posición de autoincriminación, ya que si no se ha desplegado actividad de investigación interna, no existirá la más que problemática cuestión de si el resultado de toda esta investigación ha de ser trasladado al Ministerio Fiscal en caso de que se llegué a la conclusión de que los hechos presuntamente son constitutivos de delito o de si, a requerimiento de un órgano judicial o fiscal, se debe de atender la remisión o no, siempre, claro está, que sea ex ante de la posible consideración de la propia persona jurídica como investigada dentro del mismo. Y, finalmente, desde la perspectiva del informante, éste no verá afectada en nada su posición.

En relación con esta cuestión, cabe plantearse también cuál será la responsabilidad del responsable del sistema interno de información en aquellos casos en que, recibiendo una información sobre hechos indiciariamente constitutivos de delito, opte por realizar una investigación interna con carácter previo a su remisión a la Fiscalía.

La primera cuestión que debe de abordarse es la relativa a que la información claramente sea de hechos presuntamente constitutivos de ilícito penal. En este supuesto el responsable del sistema estaría incumpliendo la obligación de remisión inmediata que establece la ley. En tal caso, la primera cuestión a valorar es la posible responsabilidad penal del mismo, pues el delito de encubrimiento sanciona, con penas de prisión de seis meses a tres años, a: el que, con conocimiento de la comisión de un delito y sin haber intervenido en el mismo como autor o cómplice, interviniere con posterioridad a su ejecución, de alguno de los modos siguientes: 1.º Auxiliando a los autores o cómplices para que se beneficien del provecho, producto o precio del delito, sin ánimo de lucro propio. 2.º Ocultando, alterando o inutilizando el cuerpo, los efectos o los instrumentos de un delito, para impedir su descubrimiento. 3.º Ayudando a los presuntos responsables de un delito a eludir la investigación de la autoridad o de sus agentes, o a sustraerse a su busca o captura, siempre que concurra alguna de las circunstancias siguientes: a) Que el hecho encubierto sea constitutivo de traición, homicidio del Rey o de la Reina o de cualquiera de sus ascendientes o descendientes, de la Reina consorte o del consorte de la Reina, del Regente o de algún miembro de la Regencia, o del Príncipe o de la Princesa de Asturias, genocidio, delito de lesa humanidad, delito contra las personas y bienes protegidos en caso de conflicto armado, rebelión, terrorismo, homicidio, piratería, trata de seres humanos o tráfico ilegal de órganos. b) Que el favorecedor haya obrado con abuso de funciones públicas. En este caso se impondrá, además de la pena de privación de libertad, la de inhabilitación especial para empleo o cargo público por tiempo de dos a cuatro años si el delito encubierto fuere menos grave, y la de inhabilitación absoluta por tiempo de seis a doce años si aquél fuera grave. (artículo 451 CP).

En palabras de la STS núm. 67/2006, de

7 de febrero, serán elementos comunes a todas ellas: a) la comisión previa de un delito; b) un segundo elemento de carácter normativo, como es el no haber intervenido en la previa infracción como autor o como cómplice, puesto que tanto el autoencubrimiento como el encubrimiento del copartícipe son conductas postdelictuales impunes; y c) un elemento subjetivo, consistente en el conocimiento de la comisión del delito encubierto, lo que se traduce en la exigencia de un actuar doloso por conocimiento verdadero de la acción delictiva previa, lo que no excluye el dolo eventual, que también satisface tal requisito y cuya concurrencia habrá de determinarse, en general, mediante un juicio de inferencia deducido de la lógica de los acontecimientos. En similares términos se pronuncia la STS núm. 178/2006, de 16 de febrero». (STS 2ª 29-1-13).

De ello se deriva que el núcleo esencial para valorar su posible responsabilidad penal partirá del grado en que se pueda afirmar el conocimiento de la comisión de un delito, pues no cabe duda que, en la mayoría de supuestos, nos encontraríamos ante un conocimiento por referencia; más no cabe descartar que, en aquellos casos, en que la información sea claramente reveladora de la comisión de un delito, con pruebas de ello, si el responsable del sistema no cumple con la obligación de remisión inmediata y, frente a ello, decide abrir una investigación interna podría estar cometiendo un delito de encubrimiento.

A partir de ahí, lógicamente, habrá de determinarse en qué consiste la investigación interna y como finaliza la misma, pues siempre es posible que, una vez realizada, ponga los hechos en conocimiento del Ministerio Fiscal con lo cual, habrá retrasado la remisión, pero no intervenido de forma sustancial a los efectos del encubrimiento. Cuestión distinta es si, tras dicha investigación, se seleccionan pruebas ocultando algunas, pues en tales supuestos, aunque posteriormente se remitan los hechos al Ministerio Fiscal, se podría haber cometido el delito.

Tales supuestos tendrán especial complejidad cuando la información que se comunique, más allá de una posible implicación delictiva de la persona denunciada, conlleve una eventual responsabilidad penal de la persona jurídica, pues se adentra en el difuso campo de la colisión de regulaciones. Por una parte, la empresa tendrá en la mayoría de los casos un sistema de cumplimiento normativo a efectos del artículo 31.bis del CP y, por otro, consecuencia de la nueva ley, tendrá implantado el sistema interno de información, pudiendo, además, coincidir en la misma persona la responsabilidad de ambos sistemas. Entiendo al respecto que lo más favorable para tal responsable, en tales casos, será la remisión inmediata al Ministerio Fiscal, pues ello conllevaría evitarse problemas de autodenuncias. Si la remisión es inmediata, sin practicar actuación de investigación alguna, se estará cumpliendo con una obligación legal, actuando como un mero cauce de transmisión entre el informante y el Ministerio Fiscal, será una traslación de la voluntad del informante al órgano competente a efectos de que éste se encuentre amparado tanto por la ley /2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción a efectos de evitar represalias, como por las normas del procedimiento penal en orden a su anonimato. No se trataría propiamente de una autodenuncia.

Cuestión diferente es que se realicen actuaciones de investigación y están pongan al descubierto, más allá del posible delito cometido por otro empleado, la eventual responsabilidad penal de la persona jurídica, pues habrá existido una recopilación de evidencias, documentales esencialmente, que, de remitirlas íntegras podrían conllevar una eventual condena. Que tal remisión sea exigible, es una cuestión que resulta más que dudosa. Pero, en cualquier caso, no se trata ahora de abordar tal cuestión, pues lo que se pretende con lo expuesto, es únicamente advertir de la posible responsabilidad penal propia del responsable del sistema en estos supuestos, pues más allá de ser un empleado de la entidad, su posición le sitúa como garante del cumplimiento del sistema.

CONCLUSIÓN

Desde una vertiente práctica, propia de la faceta profesional, la nueva normativa ha establecido un nuevo sistema que deberá de convivir con la normativa derivada de los programas de cumplimiento normativo y con la obligación ex lege de puesta en conocimiento al Ministerio Fiscal de los hechos cuando indiciariamente se aprecien indicios de delito. Optando, desde una perspectiva subjetiva, por la conveniencia de que tal puesta en conocimiento sea pauta general y no excepción, a efectos de evitar problemas procesales y, puede, materiales, de incierta resolución.

IMPLICACIONES DE LA LEY DE PROTECCIÓN DEL DENUNCIANTE EN EL DERECHO A NO INCRIMINARSE DE LAS PERSONAS JURÍDICAS

Oliver Pascual Suaña
Abogado en Muro & San Juan
Doctor en Derecho
Profesor asociado Derecho Procesal Universidad de Valladolid (UVA)

INTRODUCCIÓN

Los comúnmente conocidos como "canales de denuncias" son un elemento clave en la prevención, detección y evitación de ilícitos, tanto en el sector público como en el privado.

Por ese motivo, en un clima de constantes escándalos como *LuxLeaks,* los Papeles de Panamá o *Cambridge Analytica*, en los que tuvo una importancia crucial el papel de los denunciantes, se inició el proceso de aprobación de un texto que abordara un marco regulatorio comunitario, que culminó con la promulgación de la Directiva (UE) 2019/1937 del Parlamento Europeo y del Consejo de 23 de octubre de 2019 relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión, conocida como *"Directiva Whistleblower"*, y así se llamará en adelante.

Con el retraso en la transposición, propio de nuestro país, se aprobó la Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción (*"Ley de protección del denunciante"*, desde ahora).

El texto español, con un ámbito de aplicación material considerablemente más amplio que el mínimo contemplado en el artículo 2 de la Directiva *Whistleblower,* supondrá sin duda un impulso definitivo para la generalización de los canales de denuncias, y la protección de los denunciantes (aspectos ambos en los que España tiene escasa tradición) pero, como se tratará en este artículo, atendiendo lo preceptuado por la Ley de protección del denunciante, el texto puede tener consecuencias perniciosas sobre el derecho a no incriminarse de las personas jurídicas. En particular, puede afectar a este derecho fundamental la obligación de informar al Ministerio Fiscal con carácter inmediato cuando los hechos conocidos mediante el canal interno de información pudieran ser indiciariamente constitutivos de delito (artículo 9.2.j), y la exigencia de contar con un registro de informaciones accesible a la autoridad judicial competente (artículo 26).

Por ello, y principalmente desde el prisma de la responsabilidad penal de las personas jurídicas, se analizarán las consecuencias negativas que la Ley 2/2023 puede tener en el derecho de defensa de los sujetos colectivos, y el posible método para su evitación.

SITUACIÓN ANTERIOR A LA ENTRADA EN VIGOR DE LA LEY DE PROTECCIÓN DEL DENUNCIANTE

Según resulta incontrovertido en la doctrina procesalista, el derecho a no incriminarse, consagrado en el artículo 24.2 de la Constitución Española tiene tres derivaciones distintas: el derecho a guardar silencio; el derecho a no declarar contra sí mismo; y el derecho a no confesarse culpable. El origen y fundamento tradicional del *nemo tenetur se ipsum accusare* – precisamente, también, el mayor obstáculo para su preconización respecto a las personas jurídicas – se ha ubicado en la evitación de torturas como método para lograr la confesión del acusado en el sistema inquisitivo. Se apunta también como justificación motivaciones de carácter religioso – *las personas solo responden ante Dios* –. Ambas posturas, sin duda, están tan relacionadas con la dignidad de la persona y su libertad individual que no resultan automáticamente extrapolables a los entes colectivos.

De este modo, su reconocimiento expreso respecto a las personas jurídicas (en los artículos 409 y 786 bis de la Ley de Enjuiciamiento Criminal) obedece principalmente al pretendido aseguramiento de dos bienes jurídicos del proceso: el derecho de defensa y la presunción de inocencia.

En la fijación de los contornos del también conocido como derecho a la no colaboración activa, ha sido decisivo el Tribunal Europeo de Derecho Humanos. Aunque esta prerrogativa no aparece expresamente contemplada en el artículo 6 del Convenio de Derechos Humanos, se considera implícitamente prevista en el mencionado precepto, como parte de la esencia de un proceso equitativo (Sentencia del Tribunal Europeo de Derechos Humanos de 3 mayo 2001, J. B. c. *Suiza*). Debe destacarse la Sentencia del Tribunal Europeo de Derechos Humanos, de 17 de diciembre de 1996, *Saunders c. Reino Unido*, en virtud de la cual se asentó el criterio de que el derecho a no incriminarse no se extiende al material que *tenga una existencia independiente de la voluntad del sospechoso*. Esta doctrina ha sido asumida por otros Tribunales, aunque con matices.

Así, para el Tribunal de Justicia de la Unión Europea, desde la Sentencia de 18 de octubre de 1989, *Orkem c. Comisión*, C – 374/87, la Comisión Europea puede, si fuera preciso, requerir los documentos correspondientes que obren en poder de la entidad investigada, incluso si los mismos pueden servir para probar contra ella o contra cualquier otra empresa la existencia de una conducta infractora, si bien, apunta que se debe respetar el derecho de defensa, por lo que no cabe imponer a la entidad la obligación de dar respuestas que impliquen admitir la existencia de una infracción cuya prueba incumbe a la Comisión Europea. Por lo tanto, para el Tribunal de Justicia de la Unión Europea, el derecho a no incriminarse habilita únicamente a no realizar manifestaciones que puedan resultar autoinculpatorias, excluyendo de su ámbito de protección los documentos que obren en poder del investigado.

El Tribunal Constitucional consolidó como criterio, en la Sentencia núm. 76/1990 de 26 abril (referida a un requerimiento de aportación de documentos contables), que su exhibición, como elemento que permite acreditar la situación económica del contribuyente ante la Administración Tributaria, es imprescindible para asegurar el cumplimiento de las obligaciones fiscales, por lo que su aportación no equivale propiamente a la emisión de una declaración autoinculpatoria que, según esta resolución, es lo que protegería el derecho previsto en el artículo 24.2 de la Constitución Española.

Por su parte, el Tribunal Supremo (por todas, Sentencia núm. 277/2018 de 8 junio), afirma que el derecho a no incriminarse protege únicamente los documentos que tienen existencia independiente de la voluntad del sujeto y, además, las declaraciones que tengan un contenido directamente incriminatorio efectuadas con carácter previo al proceso, o durante el mismo, obtenidas mediando coacción.

Este cuerpo jurisprudencial se ha interpretado de tal forma que aquellos documentos que vengan exigidos *ex lege*, no estarían protegidos por el derecho a la no colaboración activa. Por lo tanto, si son requeridos por la autoridad administrativa o judicial, el sujeto compelido, persona física o jurídica, estará obligada a su aportación. El ejemplo más paradigmático sería la contabilidad societaria, exigida por el artículo 25 del Código de Comercio, y que por lo tanto deberá ser entregada por la persona jurídica incluso aunque su contenido no favorezca su posición en el proceso penal, u administrativo sancionador.

La doctrina que se ha esbozado brevemente resulta decisiva para el enjuiciamiento de las personas jurídicas. La documentación es el soporte vital de su vida diaria y, con ello, elemento clave en su enjuiciamiento. Muestra de ello es el artículo 554 de la Ley de Enjuiciamiento Criminal, que en buena medida liga el domicilio de las personas jurídicas, su conceptuación, al lugar en que se encuentran sus documentos. Por ello, puede afirmarse que el proceso penal es una pugna por *los papeles*: la acusación, que pretenderá incorporar todos los documentos posibles de la persona jurídica investigada: y la defensa, buscando que accedan al proceso solo aquellos soportes que no favorezcan su propia incriminación.

AUTO DE LA SALA DE LO PENAL DE LA AUDIENCIA NACIONAL (SECC. 4), NÚM. 391/2021 DE 1 DE JULIO DE 2021. EL "CASO ABENGOA"

Exponente de la doctrina *Saunders,* en el ámbito de las personas jurídicas, es el Auto de la Sala de lo Penal de la Audiencia Nacional (Sección 4), núm. 391/2021 de 1 de julio.

La resolución tiene su origen en el proceso seguido ante el Juzgado Central de Instrucción número 2 de la Audiencia Nacional, conocido como "Caso Abengoa", relativo a un supuesto delito de falseamiento de las cuentas anuales de la Sociedad andaluza, de los ejercicios 2013 a 2016, conducta típica prevista en el artículo 282. bis del Código Penal.

En el seno de esas diligencias, el instructor, en fecha 10 de mayo de 2021, dictó una Providencia por la que requería a ABENGOA, para que aportara en lo siguiente:

"la totalidad de las denuncias internas de ABENGOA 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."

Ante tal requerimiento, la defensa formuló el correspondiente recurso de apelación ante la Sala de lo Penal de la Audiencia Nacional, la cual dictó el ya referido Auto núm. 391/2021 de 1 de julio.

La Sala de lo Penal de la Audiencia Nacional, partiendo precisamente de la jurisprudencia del Tribunal Europeo de Derechos Humanos, recordó:

"En materia de requerimientos de documentación a personas jurídicas habrá que distinguir (…) aquellos referidos a materiales cuya existencia tiene un carácter obligatorio ex lege y, por tanto, independiente de la voluntad del sujeto en cuestión que estarían excluidos del ámbito de protección del derecho a la no autoincriminación"

Por ello, concluye la resolución:

"Desde la dificultad que entraña, deslindar aquellos documentos de la persona jurídica cuyo origen puede relajar la aplicación del derecho fundamental a no autoincriminarse, el Tribunal entiende que estarían amparados por aquél, los documentos internos procedentes del "canal de denuncias" de las empresas en los que consten los hechos denunciados y los resultados de las investigaciones internas que, voluntariamente haya llevado a cabo la entidad, así como cualesquiera declaraciones bien de la entidad, o de sus representantes legales, admitiendo la existencia de irregularidades o ilegalidades en su actuación corporativa."

En definitiva, estaba claro, al menos hasta la Ley de protección del denunciante, que la información obrante en el canal de denuncias, compuesto tanto por las denuncias recibidas, como por las indagaciones internas realizadas en su virtud, estaba absolutamente protegido por el derecho a no incriminarse de las personas jurídicas.

LEY 2/2023, DE 20 DE FEBRERO, REGULADORA DE LA PROTECCIÓN DE LAS PERSONAS QUE INFORMEN SOBRE INFRACCIONES NORMATIVAS Y DE LUCHA CONTRA LA CORRUPCIÓN.

Este panorama puede haber sufrido un reciente cambio, a resultas de la Ley 2/2023, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción.

La norma española tiene el objetivo de proteger a los ciudadanos que en un contexto laboral o profesional detecten infracciones penales o administrativas graves o muy graves, o que, en su caso, afecten al Derecho de la UE, y las comuniquen mediante los mecanismos contemplados en el texto, esto es, canales internos, externos, o revelaciones públicas. La Ley de protección del denunciante se inserta igualmente en la tendencia legislativa hacia el fomento de la autorregulación empresarial, inercia que tuvo como mayor exponente la instauración de la responsabilidad penal de las personas jurídicas.

El mecanismo principal ("preferente", según la Ley) para la formulación de las denuncias es el sistema interno de información, cauce para poner en conocimiento de la propia organización las infracciones detectadas. El sistema interno, cuya principal herramienta será el canal de denuncias, deberá facilitar un uso asequible, garantizar la confidencialidad de las informaciones recibidas, y respetar las mejores prácticas en seguimiento de las denuncias, investigación de las infracciones delatadas, y protección de los informantes. La gestión del canal podrá ser externalizada parcialmente, encomienda para la que el perfil ideal es el de un abogado, como luego se desgajará. La obligación de contar con sistemas internos de información se extiende a todas las entidades que integran el sector público y, en el sector privado, las personas físicas o jurídicas que tengan contratados cincuenta o más trabajadores. La Ley contempla dos plazos máximos para que las entidades se adapten a sus exigencias. Las Administraciones, organismos, empresas y demás entidades obligadas a contar con un Sistema interno de información tenían hasta el 13 de junio de 2023 para implantarlo. Por su parte, las entidades jurídicas del sector privado con doscientos cuarenta y nueve trabajadores o menos, así como de los municipios de menos de diez mil habitantes, tendrán hasta el 1 de diciembre de 2023.

El incumplimiento de la obligación de instaurar un sistema interno de información puede ser castigado con multas que van desde 600.001 a 1.000.000 euros, en el caso de las personas jurídicas.

Como segundo cauce, la Ley contempla la creación de la Autoridad Independiente de Protección del Informante (A.A.I) o, en su caso, entidades análogas a nivel autonómico, que tendrán como principal función la gestión de los canales externos de información. Mediante los canales externos, se podrán denunciar las infracciones detectadas en entornos laborales que entren dentro del ámbito de aplicación de la Ley de protección del denunciante.

El tercer medio de comunicación de infracciones son las revelaciones públicas, definidas como la puesta a disposición del público de información sobre acciones u omisiones que constituyan la infracción del ámbito material contemplado en la Ley de protección del denunciante. No obstante, como exige el artículo 28, para que los informantes que utilicen la vía de la revelación pública estén dotados de protección, es preciso que hayan intentado previamente la comunicación por canales externos o internos, sin que estos hayan tomado medidas; que se tengan motivos razonables para creer que la infracción pueda constituir un peligro inminente o, en su caso, que exista un elevado riesgo de represalias o pocas probabilidades de que se otorgue un tratamiento efectivo a la información debido a las circunstancias particulares del caso.

Las concretas medidas de protección a los informantes se recopilan en el Título VII de la Ley, teniendo como objetivo primordial la prohibición de represalias, entendiendo por tales cualesquiera actos u omisiones que estén prohibidos por

la ley, o que, de forma directa o indirecta, supongan un trato desfavorable. Se considerarán represalias frente a los denunciantes actos de la empresa como el despido o la modificación sustancial de las condiciones de trabajo, entre otras. La Ley contempla igualmente lo que denomina medidas de apoyo, pudiendo referir aquí la información y asesoramiento integral, accesible y gratuito, sobre los procedimientos y recursos disponibles, para la protección frente a represalias y sobre los derechos del informante; la asistencia jurídica; o el apoyo financiero o incluso psicológico, si así lo aconsejara la A.A.I. Como medidas de protección frente a represalias, debe destacarse que en los procesos judiciales civiles o laborales, incluidos los relativos a difamación, violación de derechos de autor, vulneración de secreto, infracción de las normas de protección de datos, revelación de secretos empresariales, o a solicitudes de indemnización basadas en el derecho laboral o estatutario, los denunciantes no incurrirán en responsabilidad de ningún tipo como consecuencia de las delaciones realizadas.

Indudablemente, la Ley de protección del denunciante va a suponer el impulso definitivo para que empresas de cincuenta o más trabajadores instauren modelos de prevención penal en los que los canales de denuncias son un elemento esencial. No obstante, va a suponer también la entrada en vigor de dos obligaciones legales relevantes, con posible incidencia en el derecho a no incriminarse: la obligación de denunciar ante el Ministerio Fiscal los delitos que hayan sido cometidos en su seno, y que sean detectados mediante el sistema interno de comunicaciones, contemplada en el artículo 9.2.j; y la obligación de contar con un registro de comunicaciones, prevista en el artículo 26.

OBLIGACIÓN DE DENUNCIAR ANTE EL MINISTERIO FISCAL (ARTÍCULO 9.2.J)

Dentro del artículo 9, nominado "procedimiento de gestión de informaciones", se recoge (apartado 2, letra j) la siguiente obligación:

"Remisión de la información al Ministerio Fiscal con carácter inmediato cuando los hechos pudieran ser indiciariamente constitutivos de delito. En el caso de que los hechos afecten a los intereses financieros de la Unión Europea, se remitirá a la Fiscalía Europea."

De este modo, cuando los canales de denuncias sirvan para detectar infracciones con encaje en algún tipo penal, la entidad estará obligada a ponerlo en conocimiento del Ministerio Fiscal.

Esta exigencia, aunque ya ínsita en la obligación de denunciar delitos públicos que prevé el artículo 259 de la Ley de Enjuiciamiento Criminal, esconde no obstante un peligro grave para el derecho a no incriminarse de las personas jurídicas cuando, tal ilícito, pudiera haberse cometido concurriendo los presupuestos para declarar también la responsabilidad penal de corporación, según el artículo 31 bis del Código Penal.

En todo caso, la previsión del artículo 9.2.j queda "desactivada" por el superior derecho a no incriminarse, pues lo contrario sería tanto como imponer una obligación de "autodenuncia" claramente inexigible por mor del artículo 24.2 de la Constitución Española.

OBLIGACIÓN DE CONTAR CON UN LIBRO – REGISTRO DE INFORMACIONES, Y DE LAS INVESTIGACIONES INCOADAS EN SU VIRTUD (ARTÍCULO 26)

El segundo precepto de la Ley de protección del denunciante que incide en el derecho a incriminarse es el artículo 26, cuyo apartado 1 señala:

"Todos los sujetos obligados, de acuerdo con lo dispuesto en esta ley, a disponer de un canal interno de informaciones, con independencia de que formen parte del sector público o del sector privado, deberán contar con un libro-registro de las comunicaciones recibidas y de las investigaciones internas a que hayan dado lugar, garantizando, en todo caso, los requisitos de confidencialidad previstos en esta ley."

Por lo tanto, ahora ya sí, existe un precepto que establece la obligatoriedad de contar con un canal de denuncias. Aplicando lo dicho hasta el momento, los canales de denuncias ya no estarían protegidos por el derecho a no incriminarse.

No obstante, según criterio del que suscribe, estaría justificado que la persona jurídica se niegue a la entrega del material recabado mediante el canal de denuncias cuando la conducta punible realizada por la persona física sea encuadrable en alguno de los delitos que, según la Parte Especial del Código Penal, pueden causar la responsabilidad criminal de las personas jurídicas.

De lo contrario, si se impusiera la entrega de los documentos aun habiendo riesgo de que ello perjudique la defensa de la corporación, estaríamos ante un auténtico "juego sucio" del Estado: *por un lado,* bajo la amenaza sancionadora, se obliga a la empresa a contar con un modelo de prevención penal, en el que los canales de denuncias son uno de los elementos troncales; *por otro,* se utilizan los documentos que ella misma ha recabado y generado para condenarla.

La obligación (o no) de entregar el registro de comunicaciones recibidas no es para nada baladí desde la perspectiva de la responsabilidad penal de las empresas y demás entes colectivos de los que puede predicarse su responsabilidad penal:

Tras la instauración en el año 2010 de la responsabilidad penal de las personas jurídicas, en el año 2015 se introdujo en el Código Penal, como causa de exoneración de responsabilidad criminal de los sujetos colectivos, la aprobación e implantación de un modelo de prevención penal que cumpliera los requisitos del apartado 5 del artículo 31 bis CP.

Como se deduce del Código Sustantivo, este instrumento debe ostentar dos grandes virtudes: idoneidad, cualidad teórica que implica, desde una perspectiva *ex ante*, su aptitud para prevenir, detectar y reaccionar frente a ilícitos penales susceptibles de ser cometidos atendiendo a las circunstancias específicas de la persona jurídica; y eficacia, con proyección ya práctica, que exige determinar si el sistema, amén de adecuado teóricamente, tiene relevancia real en el funcionamiento diario de la sociedad, permitiendo mitigar o eliminar los riesgos de comisión delictiva.

En este sentido, la *Guía para la evaluación de programas de cumplimiento,* elaborada por el Departamento de Justicia de los Estados Unidos, señala entre los aspectos a evaluar para determinar si el programa de *compliance* funciona en la práctica, la respuesta que haya dado la corporación a las infracciones detectadas previamente mediante el canal de denuncias.

Partiendo de lo antedicho, y desde el punto de vista de la eficacia del modelo de prevención penal de las personas jurídicas, tanto el contenido de las denuncias recibidas, como el producto de las investigaciones internas resulta esencial para la acreditación de la eficacia del *compliance program*.

Si se atestigua que el canal de denuncias ha posibilitado la reacción corporativa frente a incumplimientos detectados, en el concreto delito investigado o en situaciones anteriores, la entidad dispondrá de un indicio palpable de la cultura de cumplimiento instaurada en su seno. Por el contrario, si con ocasión de un proceso penal se pone de manifiesto que la corporación no ha respondido ante denuncias por ilícitos de naturaleza similar a los que son objeto del procedimiento, en la práctica, se imposibilitará la exoneración de responsabilidad de la persona jurídica.

De este modo, la accesibilidad a las autoridades del registro de comunicaciones de la entidad puede terminar siendo la mejor evidencia para acreditar la vulnerabilidad del modelo de prevención penal, de ahí el grave peligro que puede generar, desde la perspectiva de la defensa corporativa, la obligación que establece el artículo 26.

EXTERNALIZACIÓN DE LA GESTIÓN DEL CANAL DE DENUNCIAS COMO MÉTODO PARA LA PROTECCIÓN DE LA INFORMACIÓN GENERADA

Constatado ya que la exigencia legal del registro de comunicaciones puede provocar que el canal de denuncias quede expuesto a los Tribunales, se va a apuntar el posible método para evitar que material tan delicado quede a merced de las autoridades.

Las investigaciones internas, realizadas a resultas de las denuncias recibidas en el canal, están íntimamente relacionadas con el derecho de defensa de la corporación.

La concepción de los canales como parte del derecho de defensa – *defensa material* – no despierta dudas: realizar una investigación interna habilita que la persona jurídica pueda construir su mejor versión de los hechos ocurridos en su seno.

Por lo anterior, está plenamente justificado, e incluso resulta recomendable que en fases anteriores al inicio de un hipotético proceso penal intervengan letrados, externos a la entidad, con las consiguientes ventajas que comporta el secreto profesional.

La participación de sujetos ajenos a la organización, en cuanto a la gestión de los canales internos, viene expresamente prevista tanto en la Directiva *Whistleblower* (artículo 8.5) como en la Ley de protección del denunciante (artículo 15 y 32), por lo que tendría absoluto amparo.

Cabe recordar que ya se suscitó la polémica sobre si, en la gestión de los canales de denuncias previstos como requisito 4 del aptdo. 5 del artículo 31 bis del Código Penal tenía cabida la externalización en su gestión.

Tal duda fue resuelta por la Circular de la Fiscalía General del Estado 1/2016 habilitando e, incluso, recomendando la contratación de profesionales ajenos a la propia estructura de la corporación. Apunta el Ministerio Fiscal que la centralización de las funciones de cumplimiento en el órgano creado al efecto no supone que todas las atribuciones deban ser realizadas por el *compliance officer* y, concretamente respecto al canal de denuncias, señala que su diligenciamiento por personas ajenas a la empresa asegura mayor independencia y confidencialidad.

En todo caso, la salvaguarda del producto de la investigación bajo el paraguas del secreto profesional y la confidencialidad abogado – cliente, requiere observar una serie de pautas de comportamiento en la gestión de las denuncias, entre las que destaca la inclusión del abogado en todos los correos electrónicos que se intercambien sobre el transcurso de la indagación interna y, además, evitar que el fruto de las pesquisas caiga en manos de terceros que no se encuentren amparados por el secreto profesional.

A MODO DE CONCLUSIÓN

La Ley de protección al denunciante contribuirá decisivamente a la lucha contra la criminalidad, tanto en el sector público como en el privado.

No obstante, el artículo 9.2j del texto, referido a la obligación de informar de las infracciones detectadas al Ministerio Fiscal y, más particularmente, el artículo 26, causan un claro peligro sobre el derecho a no incriminarse, al provocar que personas jurídicas que aparezcan como sujetos pasivos de un proceso penal se pueden ver compelidas a aportar documentos que contribuyan a su propia condena.

A expensas de la interpretación que nuestros Tribunales otorguen a esta confrontación (derecho a no incriminarse de la persona jurídica Vs. obligación de registro de comunicaciones, y su entrega a los Juzgados), la única manera de proteger el resultado de las indagaciones corporativas será que, desde la misma recepción de las denuncias, intervengan letrados externos que permitan salvaguardar las comunicaciones de infracciones, y el producto de las investigaciones internas, bajo las ventajas del secreto profesional.

SOBRE EL CRECIENTE USO DE LA INTELIGENCIA ARTIFICIAL EN LOS ÁMBITOS POLICIAL Y JUDICIAL

Miguel Ángel Presno Linera
Catedrático de Derecho constitucional de la Universidad de Oviedo
Autor del libro Derechos fundamentales e inteligencia artificial (Marcial Pons, 2022)

Es bien conocido que los sistemas de inteligencia artificial (IA en lo sucesivo) ya se están aplicando en el ámbito de las investigaciones policiales para tratar de anticiparse a la comisión de posibles delitos y, en su caso, adoptar medidas preventivas limitativas de la libertad personal, bien sea atendiendo a criterios geográficos *(PredPol, CompStat…)*, sistemas muy frecuentes en Estados Unidos o a ciertas circunstancias personales, familiares…, como el español *VioGén*. Y es que, como señala Miró Llinares (2019, 100), "hoy, y en parte gracias a las expectativas que parece dar la IA, la sociedad no espera sólo que la policía reaccione a los accidentes de tráfico, a los hurtos en los lugares turísticos o a los altercados y agresiones violentas relacionadas con manifestaciones deportivas o políticas, sino que no sucedan, que se intervenga incluso antes de que acontezcan… en parte esto se debe al *hype*, en el sentido de altísima esperanza, en lo que se denomina el *Predictive policing* que, a su vez, nace de la fusión entre las técnicas criminológicas del análisis delictivo, las herramientas actuariales de valoración del riesgo y la IA".

El problema surge cuando estos sistemas se apoyan en datos que pueden reflejar, de manera intencionada o no, sesgos en función de cómo se registran los delitos, qué delitos se seleccionan para ser incluidos en el análisis o qué herramientas analíticas se utilizan, pudiendo generar una retroalimentación en la que, al menos en no pocas ciudades de Estados Unidos, la geografía -las zonas donde se concentra la vigilancia policial para prevenir delitos o reaccionar rápidamente ante ellos- puede operar, en palabras de O'NEIL (2018, 110), como "un valor sustitutivo altamente eficaz para la raza".

La Resolución del Parlamento Europeo, de 6 de octubre de 2021, sobre la inteligencia artificial en el Derecho penal y su utilización por las autoridades policiales y judiciales en asuntos penales (2020/2016(INI)), concluyó que los sesgos pueden ser inherentes a los conjuntos de datos subyacentes, especialmente cuando se emplean datos históricos, introducidos por los desarrolladores de los algoritmos o generados cuando los sistemas se aplican en entornos del mundo real y señaló que los resultados de las aplicaciones de inteligencia artificial dependen necesariamente de la calidad de los datos utilizados y que estos sesgos inherentes tienden a aumentar gradualmente y, por tanto, perpetúan y amplifican la discriminación existente, en particular con respecto a las personas pertenecientes a determinados grupos étnicos o comunidades racializadas.

Se destaca, igualmente, que las predicciones de IA basadas en las características de un grupo específico de personas acaban amplificando y reproduciendo formas de discriminación existentes; considera que deben hacerse grandes esfuerzos para evitar discriminaciones y

prejuicios automatizados y pide que se establezcan salvaguardias adicionales sólidas en caso de que los sistemas de IA de las autoridades policiales y judiciales se utilicen en relación con menores (párrafos 8 y 9).

En segundo lugar, y muy relacionado con lo dicho, está el recurso a la IA en el ámbito de justicia -IA judicial- para, por ejemplo, apoyar la toma de decisiones sobre prisión provisional o libertad condicional. A este respecto, la citada Resolución del Parlamento Europeo considera (párrafos 3 y 4), habida cuenta del papel y la responsabilidad de las autoridades policiales y judiciales y del impacto de las decisiones que adoptan con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, que el uso de aplicaciones de IA debe clasificarse como de alto riesgo en los casos en que tienen potencial para afectar significativamente a la vida de las personas y que toda herramienta de IA desarrollada o utilizada por las autoridades policiales o judiciales debe, como mínimo, ser segura, robusta, fiable y apta para su finalidad, así como respetar los principios de minimización de datos, rendición de cuentas, transparencia, no discriminación y explicabilidad y su desarrollo, despliegue y uso deben estar sujetos a una evaluación de riesgos y a una estricta comprobación de los criterios de necesidad y proporcionalidad, debiendo guardar proporción las salvaguardas con los riesgos identificados (Ortiz de Zárate, 2022, 333). La confianza de los ciudadanos en el uso de la IA desarrollada y utilizada en la Unión está supeditada al pleno cumplimiento de estos criterios.

A este respecto, y por aclarar de qué hablamos cuando hablamos de explicabilidad, conforme a las Directrices éticas para una IA fiable del Grupo de expertos de alto nivel sobre inteligencia artificial de la Unión Europea, "la explicabilidad es crucial para conseguir que los usuarios confíen en los sistemas de IA y para mantener dicha confianza. Esto significa que los procesos han de ser transparentes, que es preciso comunicar abiertamente las capacidades y la finalidad de los sistemas de IA y que las decisiones deben poder explicarse -en la medida de lo posible- a las partes que se vean afectadas por ellas de manera directa o indirecta. Sin esta información, no es posible impugnar adecuadamente una decisión. No siempre resulta posible explicar por qué un modelo ha generado un resultado o una decisión particular (ni qué combinación de factores contribuyeron a ello). Esos casos, que se denominan algoritmos de «caja negra», requieren especial atención. En tales circunstancias, puede ser necesario adoptar otras medidas relacionadas con la explicabilidad (por ejemplo, la trazabilidad, la auditabilidad y la comunicación transparente sobre las prestaciones del sistema), siempre y cuando el sistema en su conjunto respete los derechos fundamentales. El grado de necesidad de explicabilidad depende en gran medida del contexto y la gravedad de las consecuencias derivadas de un resultado erróneo o inadecuado".

Volviendo a la mencionada Resolución del Parlamento Europeo, en ella se insiste en que el enfoque adoptado en algunos países no pertenecientes a la Unión en relación con el desarrollo, el despliegue y el uso de tecnologías de vigilancia masiva interfiere de manera desproporcionada con los derechos fundamentales y, por lo tanto, no debe ser seguido por la Unión; destaca, por tanto, que también deben regularse de manera uniforme en toda la Unión las salvaguardias contra el uso indebido de las tecnologías de IA por parte de las autoridades policiales y judiciales, y subraya el impacto del uso de herramientas de IA en los derechos de defensa de los sospechosos, la dificultad para obtener información significativa sobre su funcionamiento y la consiguiente dificultad para impugnar sus resultados ante los tribunales, en particular por parte de las personas investigadas (párrafos 7 y 10).

En suma, en la Resolución se considera esencial, tanto para la eficacia del ejercicio del derecho de defensa como para la transparencia de los sistemas nacionales de justicia penal, que un marco jurídico específico, claro y preciso regule las condiciones, las modalidades y las consecuencias del uso de herramientas de IA en el ámbito de las actuaciones policiales y judiciales, así como los derechos de las personas afectadas y procedimientos eficaces y fácilmente accesibles de reclamación y recurso, incluidos los recursos judiciales. Subraya, además, el derecho de las partes en un procedimiento penal a tener acceso al proceso de recopilación de datos y a las evaluaciones conexas realizadas u obtenidas mediante el uso de aplicaciones de IA; destaca la necesidad de que las autoridades de ejecución participantes en la cooperación judicial, al decidir sobre una solicitud de extradición (o entrega) a otro Estado miembro o a un tercer país, evalúen si el uso de herramientas de IA en el país solicitante podría comprometer manifiestamente el derecho fundamental a un juicio justo; pide a la Comisión que elabore directrices sobre cómo llevar a cabo dicha evaluación en el contexto de la cooperación judicial en materia penal; insiste en que los Estados miembros, de conformidad con la legislación aplicable, deben velar por la información de las personas que sean objeto de aplicaciones de IA utilizadas por parte de las autoridades policiales o judiciales (párrafo 14).

Por lo que respecta a las decisiones judiciales, la IA "ya está ahí" pero, sobre todo, va a estarlo de manera cada vez más relevante pues, no en vano, las posibilidades que se abren en este ámbito son verdaderamente enormes: en ejecución de deudas, en asuntos como la elección de recursos en los países cuyos tribunales supremos dispongan del llamado certiorari, y que es una selección de asuntos en función de criterios de relevancia de la decisión, fundamentalmente para la formación de jurisprudencia; en materia de admisión de las pruebas, sobre todo en el proceso civil, donde los asuntos muchas veces hacen previsible que las únicas relevantes sean

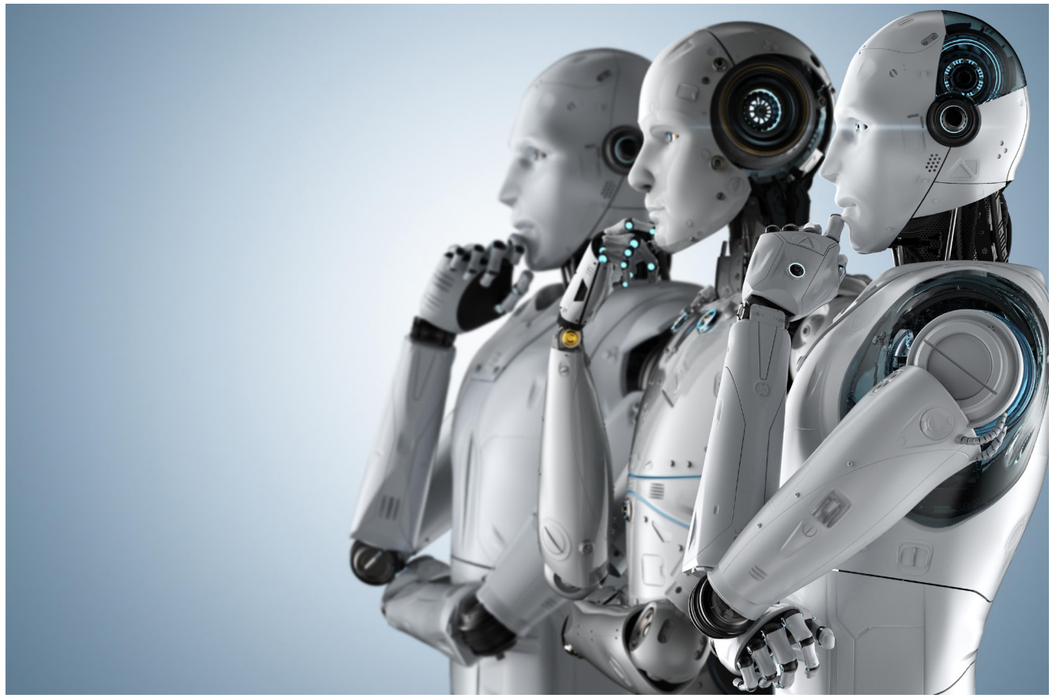
la pericial y la documental (Nieva Fenoll, 2018; 2021, 153-172; 2022, 53-68).

La cuestión esencial no es, por tanto, la presencia de la IA relacionada con el derecho de acceso a la justicia sino en cómo está articulada dicha presencia y, en particular, en qué aspectos de los procesos penales cabe acudir a ella para que no resulten menoscabados derechos como el de defensa y el de presunción de inocencia; en particular, de las personas más vulnerables.

A este respecto, y como ya se ha dicho, la Resolución del Parlamento Europeo, de 6 de octubre de 2021, recuerda que, en virtud del Derecho de la Unión, una persona tiene derecho a no ser objeto de una decisión que produzca efectos jurídicos que la conciernan o la afecte significativamente y que se base únicamente en el tratamiento automatizado de datos y pide a la Comisión que prohíba el uso de la IA y las tecnologías conexas para proponer decisiones judiciales y, como ya anticipamos, en dicha Resolución toda herramienta de IA desarrollada o utilizada por las autoridades policiales o judiciales debe, como mínimo, respetar los principios de rendición de cuentas, transparencia, no discriminación y *explicabilidad* (párrafo 4).

Y en la Propuesta de Reglamento por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) se postula (p. 33) que se consideren de alto riesgo ciertos sistemas de IA destinados a la administración de justicia y los procesos democráticos, dado que pueden tener efectos potencialmente importantes para la democracia, el Estado de Derecho, las libertades individuales y el derecho a la tutela judicial efectiva y a un juez imparcial. En particular, a fin de evitar el riesgo de posibles sesgos, errores y opacidades, procede considerar de alto riesgo aquellos sistemas de IA cuyo objetivo es ayudar a las autoridades judiciales a investigar e interpretar los hechos y el Derecho y a aplicar la ley a unos hechos concretos.

En suma, en este ámbito, ni se trata de confiar todo a la IA algorítmica ni de rechazar radicalmente lo que puede aportar, si bien aquí la explicabilidad resulta, si cabe, más irrenunciable, "tanto porque el sistema de justicia penal está basado en la argumentación y la justificación, como porque el constructo esencial configurador de responsabilidad en este ámbito es la peligrosidad que ello obliga a individualizar y no objetivar y generalizar factores y variables, por lo que resulta esencial que todos los algoritmos que aporten información de pronósticos para tomar decisiones que afecten a derechos se construyan como herramientas complementarias y de apoyo, y eviten caer en el «cum hoc ergo propter hoc» y se acerquen muchos más a modelos explicativos y argumentativos a partir de inferencias causales" (MIRÓ LLINARES/CASTRO TOLEDO, 2022, 524).



LA TEORIA DE LOS DERECHOS ETOLOGICOS Y EL COMPLIANCE

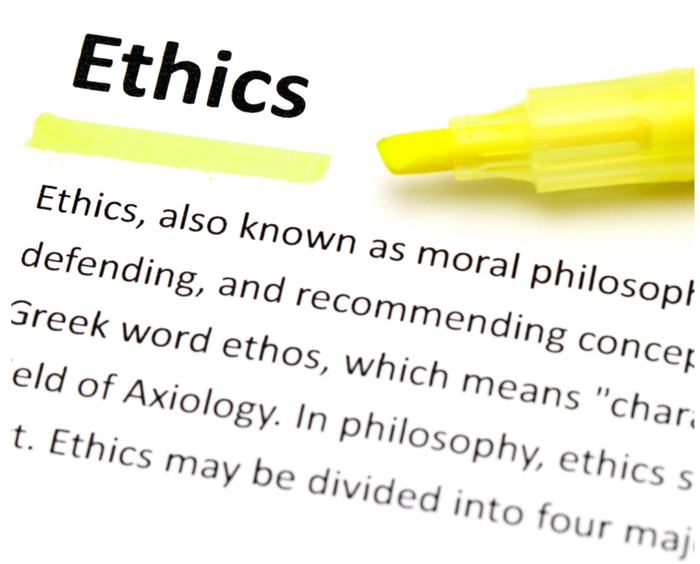
Oscar Germán Vázquez Asenjo
Doctor en Derecho
Registrador de la propiedad

PRESENTACIÓN

En este artículo, se trata de presentar las posibles utilidades que para la figura del Compliance puede ofrecer su consideración dentro de la novedosa teoría de los derechos etológicos.

El Compliance se define, en términos generales, como la acreditación del cumplimiento normativo a través de la realización de buenas prácticas, y desde un punto de vista etológico como la apreciación de un comportamiento adecuado dentro de una situación jurídica etológica de la que se deriva, como derecho etológico, la inmediata obtención de los beneficios derivados de la normativa que regula dicha situación jurídica.

Con el presente trabajo se pretende realizar un análisis introductorio y general de las posibles afinidades que conceptualmente puedan existir entre la figura del Compliance y la teoría de los derechos etológicos, tal es la razón de la ausencia de referencia alguna en estas páginas a legislación, jurisprudencia o doctrina relacionadas.



El Compliance es una figura que goza de una naturaleza jurídica de origen sajón la cual, para incardinarse dentro de la teoría general de nuestro Derecho, claramente de orden o naturaleza continental, (una troncalidad eminentemente romana, aunque mestizada en numerosos casos y materias con principios jurídicos de raíz germánica) precisa la asignación del lugar concreto que le corresponde dentro del proceso de transformación en que consiste la ciencia del Derecho y la descripción de la función que desempeña.

El Compliance pretende el cumplimiento normativo a partir de la realización de buenas prácticas con la finalidad de evitar las consecuencias indeseadas que se puedan derivar de un supuesto incumplimiento.

En realidad, el cumplimiento normativo en que consiste el Compliance carece de posible encaje general dentro de la teoría de los derechos subjetivos que ahora analizaremos. Se trata de una más de las múltiples figuras jurídicas surgidas en la actualidad que no encuentran acomodo en la teoría clásica que sistematizara Savigny, allá a mediados del siglo XIX.

El hecho de que esto sea así, impide la aplicación normal y generalizada del Compliance, es decir, mientras no hagamos encaje de su significado y efectos dentro de nuestro ordenamiento general, su utilización habrá de ser reconocida, prácticamente caso a caso, por normas específicas concretas, tantas como supuestos de hecho sean susceptibles de contar con esta particular forma de "cumplimiento normativo".

En cambio, la acreditación de buenas prácticas como forma de evitar las consecuencias negativas derivadas de un posible incumplimiento normativo podría ser una fórmula de general aplicación si lográsemos ubicarla dentro del general esquema jurídico por el cual nos regimos.

Por otro lado, en cuanto a su significado jurídico, el Compliance parece una figura perteneciente más al Derecho público que al privado, puesto que en definitiva se trata de dar cumplimiento a una normativa y no a un negocio o a un contrato. Hay en el fondo de esta figura un cierto aroma a justificar anticipadamente el cumplimiento de una normativa legal de carácter público (deberes laborales, administrativos o fiscales) y evitar así las consecuencias negativas derivadas de un posible incumplimiento (multas o sanciones varias).

Pero, más allá de esta impresión general ¿sería posible aplicar el Compliance a los derechos subjetivos que operan en las relaciones jurídicas? ¿Sería posible realizar buenas prácticas que implicasen el cumplimento de lo acordado en una compraventa o en una donación, por ejemplo?

Los ejemplos expuestos (venta o donación) nacen de la voluntad humana, son derechos subjetivos cuyo ejercicio o cumplimiento se encuentra legalmente previsto, es concreto y tiene carácter y efectos inmediatos. No se adivina qué función puede desempeñar el Compliance en el entorno de estas figuras clásicas.

En cambio, la demostración del cumplimiento de lo pactado a través de conductas o resultados directos o indirectos que lo abarquen o deductivamente impliquen el resultado perseguido sí que puede ser de aplicación a cierto tipo de derechos que, sin llegar a ser derechos subjetivos por no tener origen estricto en la voluntad del individuo, nacen del comportamiento propio de la personalidad humana.

Son los que vendremos a denominar como derechos etológicos. En ellos, el cumplimiento de los objetivos de la situación jurídica de la que emanan justifica la recepción del beneficio por parte del sujeto que ejercita un comportamiento, sin que este haya de realizar probatura alguna de su merecimiento.

TEORIA TRADICIONAL DE LOS DERECHOS SUBJETIVOS Y LA NUEVA TEORIA ETOLOGICA

El Derecho es una herramienta o instrumento producto de la personalidad humana que cada individuo utiliza para satisfacer necesidades de tipo jurídico (es decir aquellas necesidades que aspiran o pretenden obtener justicia y seguridad).

Esta herramienta consiste en un proceso de transformación compuesto de tres fases:

- **Fase inicial o fase de entrada**, en la que se produce el tratamiento inicial del hecho jurídico exteriorizado por su titular a través de la figura del acto jurídico en el marco de una relación jurídica.
- **Fase central, motor de la transformación:** se subsume el supuesto de hecho en la norma jurídica positiva y se generalizan, a través de esa norma positiva, los efectos que se hayan de producir.
- **Fase final o de salida:** la transformación operada da como resultado un producto de naturaleza plena y exclusivamente jurídica, el derecho subjetivo, que el individuo a quien se le reconozca podrá ejercitar para la satisfacción de la necesidad origen del procedimiento.

Cada una de estas tres fases aparece tradicionalmente estructurada en diferentes figuras doctrinales clásicas, que son las siguientes:

En la fase inicial o de entrada se distinguen varias figuras jurídicas.

- **Hecho natural:** cualquier hecho de la naturaleza ajeno a la participación humana
- **Hecho jurídico:** aquel hecho o acontecimiento dotado de efectos jurídicos.
- **Acto jurídico (en sentido amplio):** aquel hecho jurídico producido por la voluntad humana declarada.

En la fase central no se aprecia figura jurídica específica alguna, ya que esta fase es de transformación pura, convirtiendo las figuras jurídicas de la primera fase o fase de entrada en las figuras jurídicas de la tercera fase o fase de salida.

En la fase final o de salida apreciamos dos grandes figuras jurídicas y una extensa clasificación ulterior derivada de la segunda.

- **Relación jurídica:** entendida en este trabajo bajo la peculiar perspectiva de efecto jurídico producido en otra / otras personas y /o en una cosa como consecuencia de la exteriorización del contenido del acto jurídico.
- **Derecho subjetivo:** conjunto de poderes o facultades jurídicas que el Derecho objetivo reconoce a una persona para la satisfacción (mediante el ejercicio o defensa de acciones o excepciones) de sus necesidades jurídicas.
- **Clasificación posterior.** Se alude a la serie de categorías sucesivas en que se descompone el derecho subjetivo: relaciones personales y reales; actos (en sentido estricto) y negocios jurídicos, contratos o convenios consensuales en el primer caso y derechos reales de uso o disfrute, de garantía u optativos en el segundo.

La construcción técnica jurídica tradicional ha demostrado su éxito y utilidad a lo largo del tiempo en la atención de necesidades jurídicas clásicas y por ello debe ser mantenida y mejorada en muchos de sus aspectos susceptibles de ello.

Sin embargo, la aparición de necesidades jurídicas nacidas directamente de la personalidad humana a través del comportamiento del individuo y no a través de su declaración de voluntad evidencian que el contenido de las figuras clásicas se encuentra en su evolución agotado y resulta insuficiente.

Con la intención de cubrir la carencia apreciada, la teoría de los derechos etológicos pretende añadir, para el supuesto de los comportamientos jurídicos a los que no se extiende la postura clásica, una estructura paralela en sus fases a la tradicional pero diferente en sus contenidos y figuras. Dicha estructura resulta ser la siguiente:

En la fase inicial o de entrada apreciamos.

- **Necesidades jurídicas:** aspiraciones del ser humano a alcanzar la justicia o la seguridad en los hechos jurídicos en los que la misma se materializa para ser percibida.
- **Hecho jurídico:** todo hecho o acontecimiento de la naturaleza donde exista aspiración humana directa o indirecta.
- **Comportamiento jurídico:** actividad o conducta continuada que es susceptible de ser apreciada por la sociedad para que el sujeto pueda aprovechar directamente los beneficios que se produzcan en la situación jurídica en la que quede engranada.

En la parte central la operación de transformación es pura y no se aprecia, como en la estructura tradicional, figura jurídica específica alguna.

Y en la fase final o de salida apreciamos dos figuras jurídicas específicas y una clasificación posterior:

- **Situación etológica:** Escenario interactivo que en cada momento ocupa un comportamiento dentro de uno o varios procesos de creación de flujos económicos beneficiosos para el sujeto que se comporta y para la sociedad.
- **Derecho etológico:** El resultado que surge de un proceso de naturaleza jurídica con un sujeto que desarrolla una actividad sobre una materia que conlleve beneficios de los que ha de participar el mismo sujeto.
- **Clasificación posterior:** La principal distinción entre los derechos etológicos es la que los clasifica entre derechos etológicos ambientales y derechos etológicos de carácter personal, según se refieran al comportamiento del hombre en la naturaleza o del hombre en sociedad.

EL "COMPLIANCE" COMO COMPORTAMIENTO JURÍDICO

El Compliance no consiste en la simple acreditación de la realización de buenas prácticas, sino que en realidad es una auténtica estrategia que abarca todo un conjunto de políticas, procedimientos y acciones que personas y organizaciones privadas, normalmente ligadas al ámbito mercantil y, cada vez más, públicas, llevan a cabo para asegurar que sus actividades se ajustan a las leyes, regulaciones, normas o estándares éticos aplicables en el ámbito de su actuación.

Hasta tal punto que se llega a elaborar el concepto "Corporate Compliance" que se define como el conjunto de procedimientos y buenas prácticas adoptados por las organizaciones para identificar y clasificar los riesgos operativos y legales a los que se enfrentan y para establecer mecanismos internos de prevención, gestión y reacción frente a los mismos.

Los riesgos a prevenir han dejado de ser los estrictamente previstos en cada normativa aplicable, se amplía el ámbito de su consideración hasta abarcar todos aquellos que llevan consecuencias como el daño reputacional, la imposición de importantes multas, las pérdidas de negocio por contratos no ejecutables o la exclusión de licitaciones o subvenciones públicas, entre otras.

Como podemos comprobar, los límites entre lo jurídico, lo social, lo empresarial incluso entre lo ético o moral resultan muy difusos en la figura del Compliance y con el paso del tiempo tienden a difuminarse aún más.

Si a pesar de esta tendencia pretendemos concretar el significado del Compliance a los efectos del presente trabajo podríamos decir que se trata de la realización de buenas prácticas acreditativas del cumplimiento de una normativa. Una forma de cumplir las leyes sin riesgo alguno de que no pueda ser así y por lo tanto una figura jurídica creadora de una situación ausente de cualquier consecuencia negativa que de tal incumplimiento pudiera derivarse. Es decir, un comportamiento que persigue la seguridad de que con el mismo se haga justicia, es decir, un comportamiento jurídico.

DIFERENCIAS DEL COMPORTAMIENTO EN QUE CONSISTE EL COMPLIANCE Y LAS DECLARACIONES DE VOLUNTAD BASE DE LOS DERECHOS SUBJETIVOS

El Compliance se muestra como un proceso de difícil encaje dentro de la teoría general de los derechos subjetivos. Ya en la primera fase del proceso de transformación jurídica hay circunstancias esenciales que impiden su armonización.

El Compliance, no consiste en un acto jurídico, sino claramente consiste en un comportamiento jurídico. Es decir, no procede de hechos jurídicos en sentido clásico (aquellos hechos creados por la voluntad del sujeto que producen consecuencias jurídicas) sino que emana de la personalidad jurídica del ser humano directamente, sin necesidad de acudir al artificio de tener que ser elaborado y

manifestado por la conciencia y voluntad humanas.

El hecho de que los efectos del Compliance se deriven del comportamiento y no de la voluntad produce las siguientes consecuencias, todas ellas en conflicto con la teoría clásica de los derechos subjetivos:

- Las buenas prácticas en que consiste el Compliance han de materializarse. Es intrascendente para esta figura que exista o no previa declaración de voluntad para reconocer su existencia (cuestión esta imprescindible en la creación de los derechos subjetivos).

- Al tratarse de un comportamiento, el Compliance no precisa ser exteriorizado o manifestado ya que en si es una figura necesariamente externa y manifiesta antes incluso del inicio de cualquier tratamiento jurídico.

- En cuanto al análisis a realizar en la fase central o de transformación jurídica, en la figura del Compliance no existe verdadera subsunción de supuesto alguno de hecho en normativa alguna bajo cuyo amparo pretenda situarse, porque en realidad el supuesto de hecho previsto por la norma es sustituido por una serie de buenas prácticas necesariamente diferentes al supuesto de hecho previsto por la norma.

- La aparición de un derecho subjetivo, tampoco se da en el Compliance ya que los beneficios de quien ejercita tal comportamiento se producen antes de la fase central de transformación jurídica.

El Compliance pasará de ser una pretensión o una aspiración a aparecer como una realidad jurídica cuando las buenas prácticas produzcan su efecto liberador apoyadas en criterios de justicia y cuando sean reconocidos sus efectos de manera completamente segura y fiable.

Esta transformación no se produce en el Compliance por reconocimiento normativo (por la subsunción del supuesto de hecho en la norma) sino por la necesaria adecuación de las buenas prácticas empleadas a los efectos de la misma (llevada a cabo dicha adecuación por la simple ponderación de los principios generales que le correspondan).

No precisa el Compliance de la parte central del proceso de transformación jurídica porque el resultado de la conducta en que consiste se produce por sí solo y resulta lógico e inevitable: Por eso, la realización de buenas prácticas no requiere la concurrencia ni el ejercicio de derecho subjetivo alguno para recoger los beneficios que de su realización se derivan, sino simplemente acreditar su concurrencia o realización dentro de una situación jurídica determinada. De la simple constatación de tal existencia nacerán derechos de tipo etológico que implicarán la percepción inmediata e informal de los beneficios correspondientes.

Podemos afirmar grandes diferencias entre los actos jurídicos en su sentido tradicional y el Compliance como comportamiento jurídico.

- **Voluntad versus comportamiento**

En los actos jurídicos entendidos en sentido amplio es precisa la concurrencia activa de la voluntad humana en el momento de su creación. En el Compliance, en cambio, basta la existencia de buenas prácticas para que produzca sus efectos.

- **Declaración de voluntad versus manifestaciones de conducta**

Un acto jurídico en sentido amplio siempre es creado por la manifestación o declaración de la voluntad de un sujeto. En cambio, el sujeto puede no tener conciencia o voluntad, no ya de la creación, sino ni tan siquiera de la existencia de la situación jurídica en la que se encuentra directa o indirectamente involucrado actuando de manera natural a través de su comportamiento. En materia Compliance esto significa que las buenas prácticas realizadas por el individuo no tienen que ser expresamente declaradas por el mismo para que se produzcan los efectos liberatorios del cumplimiento de la norma.

- **El establecimiento de relaciones versus el reconocimiento de situaciones**

La consecuencia lógica de una declaración de voluntad por parte del individuo que la realiza, es la creación de una relación con otra u otras personas, aquellas a quienes va dirigida. En cambio, la consecuencia lógica del comportamiento jurídico en que consiste el Compliance no es la creación de relaciones jurídicas sino, el reconocimiento de hallarse encajado dicho comportamiento en el engranaje de una situación jurídica preexistente.

La situación jurídica, en su estructura etológica (dentro de la cual funciona el Compliance), hemos dicho que se corresponde en la clasificación clásica con la figura de la relación jurídica; sin embargo, las diferencias entre ambas figuras jurídicas son numerosas. Esencialmente se trata de conceptos distintos. Así, mientras que la relación jurídica se limita a las cuestiones de comunicación entre el sujeto activo y pasivo de esa relación, la situación jurídica abarca muchas más funciones que la relación jurídica, de tal manera que el Compliance no solo es resultado de un comportamiento o actividad, sino que es el resultado de un comportamiento entendido como parte de una situación o entorno jurídico.

- **La contraposición entre los conceptos de acción versus actividad**

En el acto jurídico el sujeto no solo ha de exteriorizar su voluntad, sino que ha de ejercitar tantas veces como sea necesario su derecho subjetivo para que los beneficios derivados del mismo puedan hacerse efectivos. En cambio, el comportamiento jurídico de una persona en el Compliance solo precisa de la existencia de una actividad, positiva o negativa por parte de esta; no existe una actuación o acción individualizada ni concreta, sino la simple actividad que se espera del comportamiento activo o pasivo de cualquier persona.

- **Derechos subjetivos versus derechos etológicos**

El Derecho transforma una relación aún no materializada en una realidad de carácter verdaderamente jurídico, es decir, transforma la manifestación de voluntad de quien ejerce un acto jurídico en una respuesta de contenido técnico-jurídico. Esto no ocurre del mismo modo con las situaciones jurídicas de las que participa el comportamiento Compliance. En estas, el resultado no podrá ser un derecho subjetivo sino más bien una figura correlativa respecto a la cual se marcan las diferencias necesarias, esto es, un derecho etológico o del comportamiento.

NOTAS CARACTERÍSTICAS DEL COMPORTAMIENTO COMPLIANCE

- **Ha de tratarse de actuaciones y no de actos**

El comportamiento Compliance al que nos referimos no puede perseguir la actuación puntual o aislada; ha de consistir en una actividad, es decir, en una reiteración periódica de actuaciones. Una de las más importantes diferencias entre los derechos subjetivos y el Compliance consiste en que los primeros se ejercitan a través de acciones/excepciones, mientras que los segundos son propios de una actividad continuada.

- **Ha de tratarse de conductas adecuadas**

El comportamiento Compliance ha de ser en todos los sentidos, adecuado; ha de engranarse de forma armónica dentro del mecanismo de una actividad general que ha de perseguir una finalidad inmaterial que resulte adecuada al ámbito de actuación al que va dirigida. El comportamiento Compliance será aquel que encaja como una pieza dentro del engranaje del entorno personal, social y ambiental en el que se encuentra.

- **Se trata de una actitud exterior por su propia naturaleza**

El comportamiento Compliance en general y la realización de buenas prácticas en particular no exigen exteriorización alguna para producir sus efectos, son externos en sí mismos, lo son hasta el punto de la imposibilidad de su interiorización o ignorancia. Esto significa que los problemas de prueba a la hora de constatar las buenas prácticas en el Compliance no deberían producirse. Independientemente de las dificultades que surjan en cuanto a la posible medición de su cuantía o calidad, deben resultar evidentes.

- **Actitudes de carácter activo.**

El comportamiento Compliance no admite pasividad o latencia alguna en su existencia. El comportamiento Compliance es activo por definición, aunque consista en un no hacer, ya que la actividad se traduce en positividad, en colaboración con la actividad general del colectivo, y no existirá esa actitud activa o positiva cuando la actuación resulte obstativa del proceso o contraria al beneficio pretendido. En el comportamiento etológico y por lo tanto también en el comportamiento Compliance no hay posibilidad de mantener actitudes pasivas, no es posible abstraerse de las circunstancias del mundo exterior. En este sentido, las consecuencias jurídicas no nacen de una relación querida y preestablecida con los demás, sino que lo hacen desde la pura acción que implica el comportamiento.

- **No existe relación con los demás en sentido clásico. Solo funciona como pieza dentro de un engranaje.**

No existe relación de persona a persona (o de persona con el colectivo). En el comportamiento Compliance, la actividad humana es un hecho cuyas consecuencias arrancan directamente de una situación consumada, relativa a la conducta como tal, desde que aparece la actividad en que se manifiesta (sin necesidad de voluntad, sin necesidad de exteriorización, sin necesidad de relación y sin necesidad de ejercicio o acción).

- **No existe criterio de reciprocidad alguno**

En el esquema clásico, las prestaciones que realiza un sujeto pueden ser llevadas a cabo por dos motivos, o bien por ánimo de liberalidad, o bien por tratar de obtener una contraprestación a cambio de la que ha consentido. Esto no es predicable del comportamiento Compliance. No se trata de que, a cambio de una actividad determinada, la sociedad o sus individuos premien por los beneficios que les supone evitar los gastos de control e inspección. Cuando las buenas prácticas encajan, pasan a formar parte de un engranaje cuyo solo funcionamiento repercute de manera general.

- **Neutralidad en su apropiación patrimonial por parte del sujeto**

La participación en el engranaje (siempre adecuada al mismo) debe constituir en sí misma un beneficio patrimonial para el sujeto que realiza el Compliance. La realización de buenas prácticas por parte del sujeto debe repercutir no solo en la liberación de un control o inspección de cumplimiento a posteriori sino en todo aquello de lo que se pueda beneficiar (ahorro añadido, prestigio reputacional, marketing, etc.).

- **El Compliance es patrimonializable**

El contenido de esta figura se puede patrimonializar, ser objeto de mercado y transacción, lo que en realidad se transmite es el valor económico que tiene el fomento de las buenas prácticas. Por eso, la patrimonialización como concepto al que nos referimos, no puede confundirse con la materialización, como cuestión que permite transformar estos valores en materiales susceptibles de cualquier tipo de transacción económica.

Este trabajo se ha realizado en el marco del proyecto de investigación "Desafíos actuales del Registro de la Propiedad: blockchain y protección de datos" (PID2020-113995CB-100), financiado por la Agencia Estatal de Investigación (10.13039/501100011033).

DISFRIMUR: UNA EMPRESA DE TRANSPORTES QUE APUESTA POR LA DESCARBONIZACIÓN Y EL COMPROMISO ÉTICO Y SOCIAL

Disfrimur es una empresa privada, española, de capital familiar, dedicada al transporte y la logística, que cuenta con una flota propia equipada con la tecnología más innovadora y que circula por todo el territorio nacional, transportando todo tipo de mercancías relacionadas con la alimentación y gran consumo.

Una empresa comprometida con sus clientes, con un **modelo de transporte, seguro, eficiente y sostenible,** y que actúa con el deseo de contribuir al desarrollo personal y profesional de sus trabajadores y respaldar su compromiso con la sociedad y el medio ambiente mediante la realización de acciones que mejoren su entorno social.

Desde 1997 trabaja dando servicios de calidad a la cadena agroalimentaria, fabricantes, distribuidores y supermercados, ofreciendo **Más transporte con Menos recursos,** basándose en la mejora continua, el aumento de la productividad y la eficacia, y siempre pensando en el mayor valor para sus clientes, con quienes mantiene una estrecha y productiva colaboración.

Para alcanzar su misión de garantizar a sus clientes una cadena logística segura, eficiente y sostenible, Disfrimur utiliza un sistema avanzado de gestión de flota, integrado con su ERP, que le permite tanto optimizar los costes como gestionar su flota de vehículos de forma eficiente.

Los gestores de tráfico de Disfrimur pueden ver desde el propio ERP la planificación y lo que está ocurriendo en la realidad con respecto a la temperatura, horarios, desvío de ruta, tráfico en tiempo real, generándose alertas y alarmas en tiempo real para poder anticiparse en caso de desviación, opciones que facilitan las tareas administrativas y de gestión al centralizar en un solo programa toda la información de los vehículos.

En busca de la eficiencia la empresa, Disfrimur desarrolla vehículos cada vez más eficientes y productivos.

Disfrimur se esfuerza por realizar un transporte cada vez más sostenible con el medio ambiente. Por ello analizan aquellas acciones que generan un gasto de combustible innecesario en el estilo de conducción de cada uno de sus conductores, se comunican y se corrigen mediante formación técnica en conducción eficiente.

Por ello, llevan más de una década trabajando con vehículos de combustibles alternativos. Disponen de vehículos de gas natural en sus dos versiones, GNC (gas natural comprimido) y GNL (gas natural licuado), vehículos eléctricos y están trabajando para incorporar próximamente otros combustibles como el biogás, el HVO y el hidrógeno.

En 2022 han afrontado **nuevos retos para seguir nuestra estrategia de transporte sostenible:**

- Electrificación de sus bases de Sangonera y San Isidro.
- Puesta en marcha de los primeros camiones eléctricos.
- Refuerzo de la energía fotovoltaica para autoconsumo.
- Seguir analizando los posibles usos del hidrógeno como combustible.
- Y el inicio del Bosque Disfrimur de 6,29 hectáreas para compensar las emisiones de CO2 en la Sierra del Molino de Calasparra, afectada por incendios en los años 2010 y 2016.

El compromiso con la sociedad de Disfrimur se concreta en colaboraciones recurrentes con ONGs y organizaciones del tercer sector, instituciones educativas como la Universidad de Murcia, etc.

En Disfrimur están especialmente orgullosos de su proyecto "Escuela de conductores", puesto en marcha junto con la colaboración de Cáritas y que cumple dos objetivos:

- Facilitar la incorporación y garantizar empleo a personas sin cualificación y/o con riesgo de exclusión social.
- Cubrir puestos de trabajo en los que la oferta sea superior a la demanda.

Finalmente cabe reseñar que Disfrimur, en su compromiso de **"tolerancia cero" con el delito** y su firme oposición a la comisión de cualquier tipo de acto ilícito o penal, aprobó en 1 de diciembre de 2017 en Junta General Extraordinaria y Universal la implantación del Programa de Prevención de Riesgos Penales para la detección, prevención y sanción de los actos y conductas fraudulentas que pudieran cometerse por parte de sus representantes legales, de quienes estén autorizados para tomar decisiones en nombre de la Empresa u ostenten facultades de organización y control de sus empleados, directivos o cualquier persona sometida a su autoridad, así como de mantener en todo momento una cultura empresarial de honestidad y ética.

DISFRIMUR

OBJETIVO
Ofrecer los servicios de transporte con la máxima calidad, al coste más competitivo y en el menor tiempo posible. Para garantizar la consecución de los mismos, la calidad y mejora continua de nuestros servicios, tenemos implantados diferentes sistemas de gestión, entre ellos ISO 9001, ISO 14001 o Compliance, que contribuyen a identificar, hacer seguimiento y mejorar las distintas áreas de la empresa para hacer realidad nuestros objetivos.

MISIÓN
Garantizar una cadena logística segura, eficiente y sostenible.

VISIÓN
Ser la mejor opción para nuestros clientes.

VALORES
Una empresa comprometida con sus clientes, con la sociedad y con su modelo de transporte, seguro, eficiente y sostenible.

En su deseo de contribuir al desarrollo personal y profesional de los trabajadores, respaldando su compromiso con la sociedad y el medio ambiente, mediante la realización de acciones que mejoren su entorno social.

REPERTORIO JURISPRUDENCIA

Por Manuel Montesdeoca de la Fuente

SENTENCIA DEL TRIBUNAL SUPREMO 1014/2022, DE 13 DE ENERO DE 20203, REC. 4912/2020

Ponente:
Sánchez Melgar, Julián Artemio.

La Sentencia resuelve el recurso de casación contra una sentencia de la Audiencia Provincial de Navarra, que condena a varias personas físicas por los delitos de apropiación indebida y falsedad documental en concurso ideal con los delitos de falsedad contable y corrupción deportiva.

La sentencia estima parcialmente los recursos interpuestos por los condenados, rebajando las penas impuestas por el delito de falsedad (al entender que los condenados no pueden ser sancionados con dos delitos en concurso) y por el delito de corrupción deportiva, así como las multas impuestas.

Tiene interés el pronunciamiento del Tribunal sobre las denominadas "primas por ganar", señalando que las mismas no pueden ser objeto de reproche penal, dado que, sin perjuicio de otras posibles consecuencias jurídicas en otros ámbitos, como el administrativo o el disciplinario deportivo, no habría una antijuridicidad material (y sí solamente formal), porque no se vulnera el bien jurídico protegido que es el "juego limpio". En definitiva, desde el punto de vista penal, tan atípicas serían las primas por ganar dadas por el propio club en el que milita el jugador, como las que ofrecerían y/o pagarían terceras personas.

En la sentencia, que tuvo (y está teniendo gran relevancia social), por haberse producido los hechos en el seno de un club de fútbol profesional (caso Osasuna), se analizan unos hechos delictivos cuyo esquema básico consistía en detraer injustificadamente cantidades importantes de dinero del club, con la finalidad de llevar a cabo compras de partidos y así evitar el descenso de categoría deportiva del club. Ante la lógica detección de las apropiaciones indebidas por los mecanismos de control externo (auditoría de cuentas), se simularon contratos y relaciones comerciales, falsificando las correspondientes facturas o recibos, que simulaban contratos de prestación de servicios o relaciones comerciales en general.

En el ámbito que ocupa a este comentario jurisprudencial, aunque no hay procesamiento ni, por tanto, condena a la persona jurídica, la Sentencia, de la que es ponente el D. Julián Artemio Sánchez Melgar, se encarga de advertir, citando la STS 192/2019, que estos comportamientos delictivos en el seno de las personas jurídicas, podrían reducirse o eliminarse mediante modelos de cumplimiento, evitando o dificultando la "autopuesta en peligro" de la persona jurídica por parte de directivos o apoderados de estas entidades.

Se trata del *"compliance ad intra"*, término ya clásico, acuñado por el Tribunal Supremo y utilizado habitualmente en las sentencias que versan sobre delitos societarios, para enfatizar la necesidad de implementar controles externos e independientes sobre la actuación de los responsables orgánicos, directivos o apoderados específicos de las empresas que tienen disponibilidad económica y de gestión y que se aprovechan de esta circunstancia para la comisión delictiva.

SENTENCIA DEL TRIBUNAL SUPREMO 89/2023, 10 DE FEBRERO, REC. 5765/2020

Ponente:
Puente Segura, Leopoldo.

La Sentencia resuelve el recurso de casación presentado por los condenados contra la sentencia de la Audiencia Nacional en el conocido como "Caso Pescanova".

A modo de resumen, de unos hechos notablemente complejos, podría decirse que los responsables y ciertos cargos ejecutivos de la entidad, con la finalidad de "ocultar" los resultados económicos adversos de varios ejercicios y asegurarse, así, el mantenimiento de la financiación externa y la entrada de nuevos inversores, diseñaron un complejo sistema de "alteración" de las cuentas, incluyendo la creación de empresas intermedias y la simulación de relaciones comerciales, para que la contabilidad reflejara resultados positivos.

En lo sustancial, la Sentencia del Tribunal Supremo mantiene la condena que la Audiencia Nacional había impuesto al presidente de la compañía, en lo relativo a los delitos de falsedad en las cuentas anuales (artículo 290 del Código Penal), en concurso medial con un delito de falseamiento de la información económica y financiera (artículo 282 bis), así como de alzamiento de bienes. Igualmente mantiene el Tribunal Supremo la condena a la mujer del presidente como cooperadora necesaria del delito de alzamiento de bienes y a ciertos directivos como cooperadores necesarios del delito de falsedad en las cuentas anuales.

El Tribunal Supremo, por el contrario, absuelve a los recurrentes del delito de falsedad en documento mercantil y de estafa agravada, por el que también les condenaba la Audiencia Nacional, al entender el Alto Tribunal que no concurre el elemento típico de la estafa; esto es, el engaño, causal al desplazamiento patrimonial, sufrido por las diferentes entidades financieras perjudicadas por el falseamiento de las cuentas.

Lo más relevante de la Sentencia que comentamos es la absolución que se acuerda tanto para el auditor externo de la compañía (Pescanova), como para la empresa de auditoría. Asimismo, se acuerda la absolución de la aseguradora de esta última, que había sido condenada por la Audiencia Nacional como responsable civil solidaria hasta el límite de la cantidad asegurada.

La importancia de la sentencia, en lo que se refiere a esta absolución, que ha sido objeto de numerosos comentarios en el ámbito del cumplimiento normativo y de la responsabilidad penal de las personas jurídicas, estriba en la doctrina, de gran importancia para la actividad de auditoría de cuentas, según la cual, no bastaría una mera conducta desatenta o negligente por parte del auditor externo de cuentas, sino que se exigiría un comportamiento doloso respecto de los delitos cometidos por la empresa auditada; es decir, una suerte de connivencia con esta última.

En relación con la aplicación del artículo 31.1 bis en la sentencia que comentamos, interesa, por último, comentar las razones esgrimidas por el Tribunal Supremo para mantener la condena a la empresa principal, estimando el recurso, sin embargo, y, por tanto, absolviendo a las personas jurídicas creadas como mero entramado de la estrategia global de encubrimiento o "falseamiento" de la situación contable.

Por lo que se refiere a la condena a Pescanova, SA, acordada por la Audiencia Nacional, el Tribunal Supremo la mantiene, desestimando el argumento que utilizaba la recurrente y que consistía en negar la obtención de beneficio o provecho, directo o indirecto de la comisión del delito. Lo relevante, por tanto, según el Tribunal Supremo, de conformidad con lo establecido en el artículo 31 bis 1, no sería si se ha producido finalmente un beneficio o provecho, sino que la conducta se haya realizado bus-

cando o pretendiendo dicho beneficio, considerado ex ante, que, como es lógico, puede frustrarse. La propia sentencia reconoce, en realidad, que se trata de una cuestión casuística, en la que deberá atenderse particularmente a cada caso para determinar la concurrencia de este elemente, que es un presupuesto para la exigencia de responsabilidad penal de las personas jurídicas.

En cuanto a la condena a las otras personas jurídicas, el Tribunal Supremo las absuelve, anulando la condena impuesta por la Audiencia Nacional, al considerarlas un mero instrumento defraudatorio; esto es, "meras coberturas formales" para eludir el pago de ciertos créditos y, por tanto, para permitir la comisión del delito de alzamiento de bienes.

Para finalizar, resulta sugestivo destacar que el Tribunal Supremo vuelve a referirse, sin desarrollarla, a la controversia sobre la responsabilidad penal autónoma o heterónoma de las personas jurídicas. En este punto, aunque la jurisprudencia sigue inclinándose por la vigencia de un sistema autónomo (volviendo a citar la clásica STS 154/2016, de 19 de febrero), en el que la ausencia de un programa efectivo de cumplimiento normativo constituye un elemento del tipo de lo injusto, parece intuirse que no es una cuestión que esté zanjada de forma definitiva.

SENTENCIA DEL TRIBUNAL SUPREMO 321/2023, DE 09 DE MAYO, REC. 1997/2021

Ponente:
Moral García, Antonio del.

La Sentencia resuelve los recursos de casación del Ministerio Fiscal y de la representación procesal de la persona jurídica que había resultada condenada por la STSJ de Madrid que, a su vez, estimaba parcialmente un recurso de apelación presentado por el Ministerio Fiscal contra la sentencia del Juzgado Mixto n.º 2 de Navalcarnero.

En la sentencia de instancia, la del TSJ de Madrid, se condena a una persona jurídica, por la comisión de un delito contra la ordenación del territorio (revocando la absolución del Juzgado Mixto) y se confirma la absolución del administrador, persona física, por ese mismo delito.

En esta sentencia hay un primer aspecto destacable, aunque no atañe a la responsabilidad de las personas jurídicas, como es el análisis de los elementos del tipo penal. En este sentido, la sentencia aclara que la comisión del delito se produce por la realización de actuaciones contrarias a la legalidad urbanística vigente, sin que pueda atenderse a una futurible o hipotética conformidad posterior con la legalidad que haya de aprobarse en algún momento futuro (que en todo caso, es incierto). Igualmente, tampoco es necesario para el reproche penal, que no haya una especial o singular afectación al territorio o los valores paisajísticos, entendiéndose que el tipo se entiende consumado por la mera vulneración de la normativa urbanística o sobre ordenación del territorio que esté vigente.

Mayo interés para el tema que nos ocupa en estos comentarios jurisprudenciales es reviste la estimación del recurso presentado por el Ministerio Fiscal contra la absolución de la persona física, administrador de la persona jurídica condenada.

El criterio del Tribunal Superior de Justicia, que viene a afirmar que solamente cabe la condena para la persona jurídica, porque los actos delictivos fueron realizados en su nombre, contradice, según el Tribunal Supremo, el sistema de responsabilidad penal de las personas jurídicas. Como argumenta el Supremo la responsabilidad de la persona jurídica es complementaria y no sustitutiva de la de la persona física. La cuestión, en definitiva, no es decidir si el sujeto responsable es la persona física, puesto que siempre, dogmáticamente, habrá una o varias personas físicas responsables (aunque a veces no sea posible su condena), sino si, además de esa o esas personas físicas, cabe también, cuando concurran los requisitos del artículo 31 bis, considerar responsable penalmente a la persona jurídica, en cuyo ámbito se ha producido el delito.

SENTENCIA DEL TRIBUNAL CONSTITUCIONAL, SALA SEGUNDA, 1/2023, 06 DE FEBRERO, REC. 2479/2019[1]

Ponente:
Tolosa Tribiño, César.

La Sentencia resuelve el recurso de amparo promovido por la Asociación Internacional Antifraude para la Defensa de los Afectados por Motores Volkswagen, representada por la procuradora de los tribunales doña María Fuencisla Martínez Mínguez y con la asistencia del letrado don Javier López Fuertes, contra los autos de 23 de noviembre de 2018 y de 14 de enero de 2019, del Juzgado Central de Instrucción núm. 2 de la Audiencia Nacional, y contra el auto núm. 104/2019, de 28 de febrero, dictado por la Sección Segunda de la Sala de lo Penal de la Audiencia Nacional

Pues bien, la Sentencia del Tribunal Constitucional 1/2023, 06 de febrero, de la que es ponente el Excmo. Sr. Don César Tolosa Tribiño, desestima el recurso de amparo promovido por la Asociación Internacional Antifraude para la Defensa de los Afectados por Motores Volkswagen con base en una presunta infracción o vulneración del derecho a la tutela judicial efectiva sobre unos argumentos coincidentes con los del Tribunal Supremo, al aludir a la mejor posición de la jurisdicción alemana para la investigación y, en su caso, sanción de los hechos.

Por una parte, no afectaría al derecho fundamental alegado como infringido la distinta naturaleza de la investigación, administrativa sancionadora en Alemania y penal en España, lo que obedece al distinto modo de estar regulada la responsabilidad de las personas jurídicas, que no puede ser penal en Alemania, pero que no presenta diferencias sustanciales en cuanto a la tipificación de la infracción, ni en la entidad objetiva del reproche jurídico (cuantía extraordinaria de la sanción), por más que su naturaleza sea conceptualmente administrativa sancionadora y no penal. En definitiva, está salvaguardado el bien jurídico protegido por más que la sanción a la persona jurídica sea administrativa y no penal, sin que, además, se excluya el riesgo de vulneración del bis in idem, como se indicaba, aunque una sanción (la que se impondría en España) fuera penal y otra, la de Alemania, fuera administrativa.

Tampoco se vulnera el derecho a la tutela judicial efectiva, que en su vertiente penal es de configuración legal, dado que es una norma de rango legal la que reconoce el derecho a promover la acción particular o popular, puesto que el ius puniendi corresponde de manera preferente y originaria al Estado.

En todo caso, la configuración legal del derecho a la tutela judicial efectiva en su dimensión penal, no impide su inclusión en el contenido esencial del derecho fundamental, sin que, en ningún caso pueda entenderse vulnerado, porque nada impide legalmente a las partes perjudicadas personarse en el procedimiento seguido en Alemania o, incluso, ejercitar en España, tras las resoluciones que se adopten en Alemania, las correspondientes acciones civiles de reclamación de responsabilidad.

[1] *En la recopilación de jurisprudencia publicada en esta misma revista, en el número correspondiente al primer semestre de 2022, comentamos la Sentencia de la Sala Segunda (Sección 1ª) del Tribunal Supremo 3449/2021, de 20 de septiembre, de la que era ponente la Excma. Sra. Dª. Ana María Ferrer García, que desestimaba los recursos de casación interpuestos por otras de asociaciones de defensa de intereses colectivos contra Autos de la Audiencia Nacional de 06 y 11 de marzo de 2019, en virtud de los cuales se acordaba la cesión de jurisdicción a favor de Alemania.*

La razón fundamental para la cesión de jurisdicción fue considerar que el mantenimiento de investigaciones separadas en España y en Alemania, ambos Estados miembros de la Unión Europea, implicaba un riesgo de vulneración del principio "non bis in ídem" prohibido `por el artículo 50 de la Carta de Derechos Fundamentales de la Unión Europea y por el artículo 54 del Convenio de Aplicación del Acuerdo de Schengen (CAAS). Un principio que, además, como ha destacado la jurisprudencia del TJUE, no se restringe a los procesos y sanciones penales stricto sensu, sino que se extiende a procedimientos y sanciones administrativas, como ocurre en este caso.

La invocación de estos preceptos se basa, lógicamente, en la acreditación como hecho probado o como premisa aceptada, de la existencia de una total identidad entre los casos enjuiciados o investigados (hasta ahora) por ambas jurisdicciones.

AUTO DE LA AUDIENCIA NACIONAL, SALA DE LO PENAL, SECCIÓN 3ª, 35/2023, DE 30 DE ENERO, REC. 427/2022

Ponente:
Rubio Encinas, Ana Mª

El Auto resuelve un recurso del Ministerio Fiscal contra el Auto del Juzgado Central de Instrucción n.º 6 de la Audiencia Nacional, de sobreseimiento provisional y archivo de una pieza de investigación penal contra varias personas físicas y dos personas jurídicas (CaixaBank y Repsol), que estaban siendo investigadas por posibles delitos de cohecho y descubrimiento y revelación de secretos.

Según el Ministerio Fiscal, en lo que atañe a las personas jurídicas, el sobreseimiento y consiguiente archivo no podía entenderse conforme a Derecho, al considerar que las personas jurídicas no contaban con un adecuado programa de prevención de delitos, que cumpliera los requisitos mínimos del artículo 31 bis y que sirviera para identificar los mencionados delitos como riesgos específicos y concretos de su actividad, ni que contara con controles eficaces para prevenir su comisión; ni generales, como el Código Ético, ni específicos.

La Audiencia Nacional desestima, sin embargo, el recurso, dando especial cuenta de los informes periciales aportados por ambas entidades para justificar la implantación en ambas del modo de prevención de delitos conforme a los requerimientos legales.

Así la sentencia en Relación al modelo de prevención penal de REPSOL que el informe del perito ratificado ante el instructor analizaba "las medidas dispuestas por REPSOL en el ámbito de la prevención de delitos corporativos y la cultura ética". Señalaba el perito que, en su análisis, había prestado especial atención a las medidas de compliance y las " directrices para la prevención de delitos corporativos que tenía implementadas REPSOL en 2011 (...) y la evolución de las medidas de compliance penal de REPSOL desde 2012 hasta la actualidad" tomando en consideración " el contexto temporal en el que se produjeron los presuntos hechos, con objeto de situar en cada momento las medidas existentes en REPSOL para la prevención y mitigación de delitos; en especial, de aquellos relacionados con la corrupción (cohecho) y el descubrimiento y la revelación de secretos".

En su informe concluía el perito que en el año 2011 la entidad REPSOL SA tenía previsto un modelo de cumplimiento y prevención de los delitos, entre los que estaban los que son objeto de este procedimiento, que era eficaz conforme a los estándares internacionales y que había diseñado, partiendo de las medidas de 'debido control' que ya tenía implementadas, creando un grupo de trabajo interno que contaba con el asesoramiento de una firma de consultoría y un despacho penalista y que tras la implementación del Modelo, REPSOL prosiguió desarrollando sus medidas de 'debido control' conforme a los principios de mejora continua del compliance en2012 y años posteriores hasta el momento analizado.

En particular, señalaba el perito, que "en 2011, el Modelo de REPSOL ya incorporaba: (i) una función/órgano de supervisión y control; (ii) la identificación de riesgos penales por actividad; (iii) políticas, procedimientos y controles; (iv) actividades de difusión, sensibilización y concienciación; (v) recursos dedicados y procedimientos específicos para la gestión de los recursos financieros; (vi) mecanismos para informar de incumplimientos(canales de denuncia); (vii) un sistema disciplinario; y (viii) la monitorización y auditoría periódica del modelo",

Añadía el perito en su informe que "(...) las medidas de control dispuestas por REPSOL permitían mitigar los riesgos penales de forma eficaz, incluyendo aquellos relacionados con la corrupción (cohecho) y el descubrimiento y la revelación de secretos. En particular, REPSOL disponía de controles específicos para mitigar riesgos de corrupción (cohecho) (72 controles) y descubrimiento y revelación de secretos (69 controles).

Estos controles (medidas de "debido control") fueron desarrollados sobre la base del sistema de control interno existente en REPSOL antes de 2011 (controles SOX y Programa de Cumplimiento Normativo). Es decir, en muchos casos, se trataba de controles maduros que venían aplicándose desde hacía tiempo y se basaban en aplicaciones nformáticas y sistemas automatizados que permitían efectuar un "debido control" y disponer de trazabilidad. Los sistemas de gestión estaban integrados y, sobre ellos, REPSOL aplicaba controles generales de ordenador, los cuales eran auditados periódicamente (.) Tras la implementación del Modelo, REPSOL prosiguió desarrollando sus medidas de "debido control" conforme a los principios de mejora continua del Compliance.

Y Entre 2012 y 2014, destacaba las siguientes actividades: (i) verificación periódica del diseño y efectividad operativa del Modelo y actividades de mejora continua; (ii) actualizaciones de la Norma de Ética y Conducta y del Reglamento de la Comisión de Ética; (iii) aprobación del Procedimiento de Seguimiento y evaluación periódica del Modelo de Prevención de Delitos (iv) aprobación de las Condiciones de uso de los canales de comunicación;(v) aprobación de la Política Anticorrupción (cuyos principios básicos ya estaban contemplados en la Norma de Ética y Conducta desde 2006); (vi) Norma de aplicación del Código de ética y conducta de proveedores; y (ix) Acciones de difusión, sensibilización y concienciación en materia de ética y prevención de delitos (...)".

En relación a CaixaBank, el Auto que comentamos - tras dar por reproducida la lista de documentos que se han analizado por el instructor y se refieren a la normativa de CaixaBank sobre Modelo de Prevención de delitos: código ético, planes de formación, canal de denuncias o régimen disciplinario, y hacer referencia a las conclusiones de la pericial del Modelo de Prevención de Delitos de CAIXABANK señalando que la entidad contaba con medidas de control adecuadas y eficaces, tanto en diseño

como en efectividad operativa, para intentar prevenir y detectar los delitos a que se refiere este informe -entre los que estaban cohecho y revelación de secretos - , sin que se hayan apreciado aspectos significativos no sometidos a dichos controles-, extrae la conclusión de que para valorar el modelo de cumplimiento de prevención de delitos han de tomarse en consideración, de forma pormenorizada los distintos controles, el ámbito en que esos controles se desenvuelven y la coherencia e interrelación de los mismos en relación con el todo, teniendo en consideración que ningún modelo es infalible, y que si un delito se comete por alguno de los sujetos previstos en el artículo 31 bis del Código Penal, eso no significa necesariamente que el modelo adoptado sea inadecuado, incumpla la normativa vigente o falle.

En definitiva, la Audiencia destaca que no hay una fórmula perfecta y eso obliga a una permanente revisión periódica del modelo de prevención de delitos, aunque alude a una serie de elementos que necesariamente deben contenerse, como el código ético, los planes de formación, el canal de denuncias o el régimen disciplinario, que evidencian la cultura de cumplimiento y prevención de delitos y respeto al Derecho implantado por la entidad.

SENTENCIA DE LA AUDIENCIA NACIONAL, SALA DE LO SOCIAL, 56/2023 DE 26 ABR. 2023, REC. 381/2022

Ponente:
Gil Plana, Juan.

La Sentencia declara nulidad de la directriz contenida en el apartado 4.3.1 del Código General de Conducta del Grupo Santander por la que los empleados deben comunicar a su responsable, Recursos Humanos y Cumplimiento & Conducta si ejerce otra actividad profesional por cuenta propia o ajena para entidades no competidoras por lesionar el derecho a la intimidad de los empleados ex artículo 18.1 de la CE.

Sostiene la parte demandante, la Federación de Sindicatos de Banca, Bolsa, Aorro, Entidades de Crédiyo, Seguros, Oficinas y despachos de la Confederación General del Trabajo (CGT), que, dada la generalidad y el carácter omnicomprensivo de esta exigencia de comunicación referida a actividades para entidades no competidoras con la actividad de la empresa demanda, se lesiona el derecho a la intimidad y el de libertad personal de los trabajadores; invocando, además, lo argumentado en la Sentencia de la Sala de 6 de marzo de 2018. En efecto, en la referida sentencia el tribunal llegó a la conclusión de que no cabía apreciar lesión de la esfera privada al establecerse que la comunicación de la realización de actividades se refería a "a la actividad de competencia o colisión con los intereses del banco y actividad paralela del empleado". Sostenía el tribunal que no había afectación del derecho de intimidad por existir un interés empresarial que venía a justificar la comunicación siempre que la actividad desarrollada por el trabajador incurriera en competencia con la de la empresa o supusiera un conflicto de intereses, lo que nos llevó al convencimiento de que aquella conducta superaba el juicio de proporcionalidad.

Sin embargo, en el presente procedimiento considera la Sala que la configuración de la comunicación es diferente y no cabe, prima facie, trasladar la misma solución. Ahora se establece, como advierte la demandante, la comunicación a la empresa de cualquier actividad para entidades no competidoras, sin establecerse restricción alguna en base a parámetros como si la entidad no competidora es proveedora o cliente de la empresa demandada o el empleado ocupa un puesto desde el cual pudiera realizar operaciones a favor de dichos proveedores y clientes en detrimento de los intereses de la empresa. Es por ello que esta Sala considera que una comunicación genérica relativa a la realización por parte de los empleados de la demandada de actividades para terceros no concurrentes con la empresa supone afectar de forma injustificada la esfera privada de los empleados, que se ven constreñidos a comunicar una faceta de su vida privada -como es la realización de actividades productivas por sí mismo o para empresas no competidoras- que es inocua a la actividad de la demanda y que ningún repercusión o perjuicio puede producir en la esfera de esta última .

Se alega por la empresa que esta obligación de comunicación incluso respecto de actividades por cuenta propia o ajena para empresas no competidoras se establece porque pueden existir conflictos de intereses en el desarrollo de esas actividades, exponiendo que un empleado puede, por ejemplo, otorgar una operación de financiación a una empresa para la que está prestando servicios. Como ya se ha indicado en el fundamento anterior, una limitación del derecho fundamental a la intimidad como la que se sostiene por la parte demandada requiere que ésta se adecúe o supere el test de proporcionalidad, y entiende esta Sala que en esta obligación de comunicación exigida a los empleados no se supera. En efecto, la comunicación a la empresa de actividades no concurrentes con la de la empresa puede ser una medida idónea para evitar posibles conflictos de intereses, es decir, superaría el juicio de idoneidad; pero no supera el juicio de necesidad porque se impone la comunicación en cualquier supuesto de ejercicio de actividades por cuenta propia o por cuenta ajena con entidades no competidoras, exista o no conflicto de intereses; existiendo, a juicio de esta Sala, otras medidas menos lesivas como sería acotar dicha comunicación cuando la actividad fuera realizada para proveedores y clientes y/o cuando el empleado, por su puesto de trabajo, pudiera estar incurso en un conflicto de intereses. Además, la comunicación exigida no es equilibrada por cuanto, para evitar posibles conflictos de intereses, se sacrifica la privacidad de la totalidad de los trabajadores de la demandada; el perjuicio que se irroga a los empleados no se justifica por el interés empresarial que se pretende salvaguardar con la referida comunicación (juicio de proporcionalidad en sentido estricto).

Por lo tanto la Sala estima que la previsión impugnada lesiona el art. 18 C.E. y condena a BANCO SANTANDER a estar y pasar por dicha declaración[2].

[2] *La Sentencia es de interés en cuanto rechaza las pretensiones de nulidad de otros preceptos del Código General de Conducta del Grupo Santander que fueron objeto de impugnación por presunta vulneración de derechos fundamentales que la Sala no considera vulnerados.*