

ENERO 2024 | 16ª 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

Pág. 04 EDITORIAL / Pág. 07 ENTREVISTA. Miguel Ángel Jimenez Velasco / **Pág.10 ARTÍCULOS.** IA y los derechos humanos en el mundo de transhumanismo / Compliance y subrogación laboral / En la sombra de las criptomonedas y del metaverso. La imperante necesidad de procedimientos internacionales contra el blanqueo de capitales en estos ecosistemas / Optimización del tax compliance a través de la IA / Los riesgos de corrupción en la fase de ejecución de la contratación pública / Qué debemos tener en cuenta para hacer negocios en latinoamérica desde la perspectiva del compliance officer / La estandarización de los procesos de investigación / **Pág. 00 EMPRESA.** full&fast, expertos en transición energética. Construyendo la empresa de servicios del futuro #chargingthefuturenow / **Pág. 51 REPERTORIO DE JURISPRUDENCIA.**

ENTREVISTA. Miguel Ángel Jimenez-Velasco

Por Luis Suárez Mariño

La opinión y experiencia de profesionales expertos en el mundo del cumplimiento es una valiosa guía para miles de profesionales y estudiantes que empiezan su andadura en el camino del compliance corporativo.



PÁG.07

ARTÍCULO. IA y los derechos humanos en el mundo del transhumanismo.

Por Manuel Lázaro Pulido

La irrupción de la inteligencia artificial es un fenómeno que ha inundado el lenguaje usado en los diversos contextos semánticos de la vida social tanto formales como informales. La inclusión de las siglas IA no pueden olvidar su entorno más amplio: el entorno digital, el espacio donde la IA trabaja con los Big Data.

PÁG.10

ARTÍCULO. Compliance y subrogación laboral.

Por Belén Luzuriaga

Cuando hablamos de Cumplimiento, sin duda, el elemento clave son las personas. Son las que hacen que en cualquier centro de trabajo se respire una cierta cultura de cumplimiento, que es la que se conforma con los valores y los principios que en una organización se consideran fundamentales.



PÁG.15

ARTÍCULO. En la sombra de las criptomonedas y del metaverso.

Por Luis Rodríguez Soler

En el universo digital de las criptomonedas y los cryptoactivos, donde la libertad financiera se entrelaza con la opacidad, o presunta opacidad de cada transacción, una amenaza persistente se esconde en las sombras: el blanqueo de capitales.

PÁG.18

ARTÍCULO. Optimización del tax compliance a través de la IA.

Por Franklin Martín Ruiz Gordillo

ChatGPT, un sistema de redes neuronales con capacidades de aprendizaje profundo que representa uno de los mayores alcances del machine Learning en materia de detección de irregularidades.



PÁG.24

ARTÍCULO. Los riesgos de corrupción en la fase de ejecución de la contratación pública

Por Joan A. Llinares

En 2022 la Agencia Valenciana Antifraude publicó una recomendación con el objetivo de alertar sobre los riesgos en la ejecución de los contratos en clave de integridad pública.



PÁG.29

ARTÍCULO. Qué debemos tener en cuenta para hacer negocios en latinoamérica desde la perspectiva del compliance officer

Por Fernando Peyretti

América Latina tiene un escenario de delitos financieros desafiante. Se identifican diferentes actividades ilícitas que a su vez están generando flujos de efectivo ilegales relacionados con los Delitos Financieros más típicos de la región.

PÁG.33

ARTÍCULO. La estandarización de los procesos de investigación. De la teoría a la metodología

Por Leocadio Marrero Trujillo

Un viaje a través del nuevo estándar internacional establecido por ISO.org bajo el nombre ISO/TS 37008:2023 Investigaciones Internas de Organizaciones: Orientación.



PÁG.38

EMPRESA. full&fast, construyendo la empresa de servicios del futuro #chargingthefuturenow

Ha desarrollado su propia tecnología de acumulación, cofinanciada por el ministerio de industria, junto con un SaaS para optimizar el consumo de energía y reducir la factura eléctrica (hasta un 70%).

PÁG.46

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.



PÁG.51

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

Uno de los fines de la AEAEC es fomentar la cultura del compliance y analizar los cambios normativos. Este ha sido siempre el objetivo de todas las actividades que hemos promovido. Por eso desde la AEAEC mostramos nuestra preocupación ante la proposición de ley de amnistía en cuanto puede suponer un uso espurio del derecho.

Cierto es que en un estado democrático la ley emana del poder legislativo que representa la voluntad de los ciudadanos representada en las urnas. Igualmente es cierto que la reciente investidura de Pedro Sánchez como Presidente del Gobierno no se puede calificar sino de legal, en cuanto que la misma ha obtenido el respaldo de la mayoría del Congreso.

Y, por supuesto, que en nuestra democracia el pluralismo político es un valor superior sobre el que se asienta el ordenamiento jurídico (art. 1 CE) y que ese pluralismo político se expresa a través de los partidos políticos, instrumentos fundamentales para la participación política, en cuanto concurren a la formación y manifestación de la voluntad popular, debiendo, por tal trascendental motivo, ser libre su creación y el ejercicio de su actividad, sin que, como defendieran, entre otros, los insignes catedráticos de constitucional, Ignacio de Otto y Juan Luis Requejo, "en nuestro ordenamiento constitucional tenga cabida un modelo de democracia militante, esto es un modelo en el que se imponga, no ya el respeto, sino la adhesión positiva al ordenamiento, y en primer lugar a la Constitución"

Desde este punto de vista la posición política de los partidos independentistas, republicanos, comunistas o ultra conservadores, no merece crítica alguna desde el constitucionalismo, siempre que su estructura interna y funcionamiento sean democráticos y sus actividades y fines no sean delictivos. Desde esta perspectiva cualquier proyecto político es compatible con la Constitución, siempre y cuando sus actividades no vulneren los principios democráticos ni los derechos fundamentales de que somos titulares todos los ciudadanos.

Lo que consideramos criticable es que un partido político, uno de los dos más importantes del Estado, con una larga trayectoria y que ha sido clave tanto en la transición democrática como en el desempeño del Gobierno durante la mayor parte de los años transcurridos desde 1978, a través del programa político con el que anunció a la ciudadanía la posición política con la que aspiraba a conseguir el apoyo de los electores, haya ocultado un tema tan trascendental como una proposición de ley orgánica de Amnistía, que aun no entrando a valorar su más que posible inconstitucionalidad formal, en cuanto supone la derogación de actos jurídicos amparados por leyes constitucionales, solo estaría justificada si persiguiese un fin constitucionalmente legítimo y se considerase proporcionada para lograr dicho objetivo.

En la Exposición de Motivos de la Ley se hace referencia de manera reiterada, y con diferentes matices a la constitucionalidad de la ley atendiendo a la

finalidad perseguida por la misma, "la consecución de un interés general, de superar y encauzar conflictos políticos y sociales arraigados, en la búsqueda de la mejora de la convivencia y la cohesión social, así como de la integración de las diversas sensibilidades políticas", o en otras palabras, "avanzar en el camino del diálogo político y social necesario para la cohesión y el progreso de la sociedad catalana" o "superar obstáculos y mejorar la convivencia avanzando hacia la plena normalización de una sociedad plural que aborda los principales debates sobre su futuro mediante el diálogo, la negociación, y los acuerdos democráticos", o "devolver la resolución del conflicto político a los cauces de la discusión política y eliminar algunas de las circunstancias que provocan la desafección que mantiene alejada de las instituciones estatales a una parte de la población" y "garantizar la convivencia dentro del Estado de derecho, y generar un contexto social, político e institucional que fomente la estabilidad económica y el progreso cultural y social tanto de Cataluña como del conjunto de España, sirviendo al mismo tiempo de base para la superación de un conflicto político".

Sin embargo, esos fines, en teoría loables, parecen contraponer el interés general, el entendimiento entre diversas sensibilidades políticas y la convivencia pacífica, con el cumplimiento de la legalidad imperante que los amnistiados vulneraron. Leyendo la exposición de motivos de la ley tal parece que la misma contrapone en definitiva la convivencia democrática con el estado democrático de Derecho, obviando en la práctica las consideraciones que ha realizado el Tribunal Constitucional sobre la amnistía, principalmente en la Sentencia del Pleno nº 147/1986, de 25 de noviembre, referida a las cuestiones de inconstitucionalidad planteadas por jueces y tribunales en relación a la Ley 1/1984, de 9 de enero, que añadía un nuevo artículo a la Ley 46/1977, de 15 de octubre, de Amnistía, concebido en los siguientes términos:

«Art. 11 bis. Las acciones para el reconocimiento de los derechos establecidos en esta Ley serán imprescriptibles. No

obstante, los efectos económicos de los derechos reconocidos estarán sujetos a las distintas normas de prescripción del ordenamiento jurídico.»

Por su parte, en la Disposición adicional de la referida Ley 1/1984, se establecía que «los interesados podrán solicitar la aplicación de la Ley de Amnistía, incluso cuando haya habido resolución judicial que declare la inadmisión del proceso por prescripción de la acción».

La conformidad de los preceptos transcritos con la Constitución suscitó dudas en diversas Magistraturas de Trabajo, que plantearon sendas cuestiones de inconstitucionalidad. Una vez acumuladas, dichas cuestiones, dieron origen a una sentencia del Pleno del Tribunal en la que se recogían consideraciones que ahora deberían de tomarse en cuenta:

- 1ª. *"Que la amnistía, fundamentándose en un ideal de justicia (STC 63/1983), pretende eliminar, en el presente, las consecuencias de la aplicación de una determinada normativa -en sentido amplio- que se rechaza hoy por contraria a los principios inspiradores de un nuevo orden político".*
- 2ª. *"Que la amnistía es una operación excepcional, propia del momento de consolidación de los nuevos valores a los que sirve, cuya finalidad unitaria no enmascara el hecho de que se pone en práctica recurriendo a una pluralidad de técnicas jurídicas que quedan unidas precisamente por la finalidad común. En unos casos normalmente para relaciones en las que el Estado aparece involucrado como poder público, la aplicación de la amnistía supondrá lo que se ha llamado por la doctrina «derogación retroactiva de normas», haciendo desaparecer por completo las restricciones que sufrió el derecho o libertad afectado, con todas sus secuelas".*
- 3ª. *"Que es claro que una institución de este género afecta a la seguridad jurídica, principio consagrado en el art. 9.3 de la C.E. Ello*

sucede porque la amnistía que se concede altera situaciones que han sido consagradas por sentencias judiciales firmes, provistas del valor de cosa juzgada (art. 118 de la C.E.), y esta alteración de las reglas de sucesión de los ordenamientos puede afectar evidentemente al principio citado, entendido como la confianza que los ciudadanos pueden tener en la observancia y el respeto de las situaciones derivadas de la aplicación de normas válidas y vigentes".

- 4ª.- *"Que la concesión de una amnistía implica un juicio crítico sobre toda una etapa histórica, eliminando los efectos negativos de cierto tipo de leyes emanadas durante su transcurso...que contrariaban derechos del hombre generalmente admitidos en el ordenamiento internacional, y hoy en el interno español."*

A la luz de dicha doctrina parece evidente que la amnistía pone cuanto menos en tela de juicio la ley aplicable a los hechos amnistiados y los valores que sustentaban aquella. Es decir que de facto la amnistía presupone la derogación de las normas que sirvieron de base para condenar los hechos amnistiado, y que esa derogación se justifica al ser las normas contrarias a los valores y principios que rigen los estados democráticos de derecho por contrariar los derechos del hombre generalmente admitidos en el ordenamiento internacional, y hoy en el interno español.

Pero, es que además resulta que las finalidades declaradas de la ley no son en realidad la causa verdadera y lícita (en nomenclatura civilista) de la mentada norma, sino una causa simulada que encubre otra cual es la necesidad de que el candidato a Presidente del Gobierno del PSOE contase con los siete votos necesarios de Junts para primero conseguir la investidura, y segundo conseguir que legislatura no se frustrase; causa que coloca al PSOE en una situación de inferioridad ante el chantaje constante del partido independentista catalán, que sabedor de la verdadera causa que inspira la ley

estira su ámbito de aplicación hasta donde le complace y solicita todo tipo de prebendas (véase el acuerdo para delegar las competencias en extranjería) sabedor de la debilidad del partido socialista que se somete voluntariamente al chantaje, concediendo sin disimulos todo aquello que le piden quienes violentaron las leyes y los valores y principios constitucionales que las sustentan.

Un estado de derecho, vá más allá del respeto a la formalidad de las leyes y la aprobación de las mismas por los legítimos representantes de los ciudadanos, y exige el respeto a los principios valores materiales recogidos en la propia Constitución, valores axiológicos que como la seguridad jurídica, la justicia, la igualdad y la separación de poderes, son fundamento del orden jurídico y la paz social.

Para garantizar precisamente que el Estado formal de Derecho sea también un Estado material de Derecho, las constituciones posteriores a la Segunda Guerra Mundial establecieron una serie de garantías y de instituciones de contrapeso, con la finalidad de asegurar que la elaboración de las leyes no respondiera tan solo a criterios democráticos sino que fueran coherentes con los principios y valores recogidos en las propias constituciones, estableciendo una vinculación entre legalidad y legitimación formal, de un lado, y estricta legalidad y legitimación sustancial, de otro, lo que exige, en palabras de Ferrajoli, que la propia ley se condicione a determinados contenidos sustanciales, que el Poder político esté limitado por el Derecho, en el sentido que caracteriza la tradición constitucional inglesa, por una parte caracterizada por la supremacía del parlamento, y por otro por el *rule of law*, entendido como *"rule or supremacy of law"*, es decir como "absoluta supremacía del Derecho que excluye la existencia de arbitrariedad o prerrogativa, o incluso amplia autoridad discrecional por parte del gobierno" e implica «la igualdad ante el Derecho, o la igual sujeción de todas las clases al Derecho ordinario del país, administrado por los tribunales ordinarios de justicia";

A mayor abundamiento las conductas que se amnistían son las realizadas por una intencionalidad política, “reivindicar, promover o procurar la secesión o independencia de Cataluña, así como todos aquellos que hubieran contribuido a la consecución de tales propósitos” obviando que mientras la Constitución ampara las conductas movidas por dicha intención, lo que no ampara es la comisión de gravísimos delitos para conseguirla. Un estado de derecho como tal basado en normas, permite adoptar decisiones tomando en consideración lo que un individuo hizo, no la intención que le movió. En definitiva, las leyes por el carácter general que las caracteriza en un estado democrático constituyen obstáculos frente a la particularización.

Un ordenamiento jurídico de un estado democrático de Derecho ha de ser predecible, y permitir que los sujetos conozcan los criterios de comportamiento conformes y contrarios a las leyes y las consecuencias que se van a derivar de la observancia o inobservancia de las mismas.

Cómo pone de relevancia Nino, citado por Requejo y otros, “existe una clara relación entre la observancia de las normas jurídicas constitucionales y el desarrollo de una sociedad, de manera que un fenómeno de ilegalidad masiva, donde concurren conductas contrarias a las normas y una determinada actitud hacia ellas, consistente en el desprecio, produce situaciones de ineficiencia y subdesarrollo”, que la amnistía de las mismas solo puede agravar.

Por último resulta preocupante, como han denunciado todas las asociaciones judiciales, la campaña preventiva iniciada contra los jueces y magistrados encargados de aplicar la ley (con señalamiento personal incluso desde la tribuna del congreso).

En la conocida y trascendental Sentencia de la Sala de lo Penal del Tribunal Supremo 154/2016, 29 de Febrero de 2016, de la que fuera ponente el que luego fuera Fiscal General del Estado, don José Manuel Maza Martín, nuestro alto tribunal equiparaba la cultura de cumplimiento

con la cultura de respeto al Derecho y ésta con la cultura ética, viniendo de algún modo a trascender el cumplimiento de la legalidad formal por a medio de un compromiso ético con el “estado material de Derecho” al que antes aludíamos.

Pues bien a nuestro humilde parecer, ni es ética la finalidad o causa real de la proposición de ley, ni es ético que se haya hurtado a los ciudadanos antes de las elecciones en el programa electoral del PSOE conocer la verdadera intención del partido, que pese a que meses antes ya sondeaba en Bruselas el camino que se apresuró a recorrer al día siguiente de conocer el resultado electoral, en campaña negó por activa y por pasiva la constitucionalidad de una amnistía reclamada por los partidos independentistas.

Estando los partidos políticos legalmente obligados a contar con programas de prevención de delitos, inspirados en la llamada “cultura ética” o de “respeto al Derecho” resulta cuanto menos llamativo que ninguno de los diputados electos haya mostrado divergencia alguna con la proposición de ley, ni con cada modificación que en el trámite parlamentario le ha exigido Junts.

La posición que dejamos expuesta no significa ningún posicionamiento político pues la AEAC no tiene ideología política alguna que aglutine a sus asociados sino la preocupación ante una proposición de Ley, preocupación por cierto compartida por insignes y acreditados socialistas, históricos dirigentes del PSOE, encabezados por quien como presidente del Gobierno de España impulsó el cambio de nuestro país, después de un golpe de Estado, hacia una homologable y moderna democracia.

ENTREVISTAMOS A MIGUEL ÁNGEL JIMENEZ VELASCO MAZARÍO

DIRECTOR CORPORATIVO DE CUMPLIMIENTO DE COXABENGOA

Por Luis Suárez Mariño

Director de European Compliance News

Licenciado en Derecho por la Universidad Autónoma de Barcelona (1989), máster en Dirección de Empresas y Finanzas por el Instituto Internacional de Empresas de la Universidad de Deusto (1990-91). Director jurídico de Abengoa desde 1996 hasta 2012. Nombrado Secretario y Letrado Asesor del Consejo de Administración y Secretario General desde 2002 hasta el 2013. Secretario de la fundación Fondo de Cultura de Sevilla (FOCUS) desde 2003 al 2013.

La opinión y la experiencia de profesionales expertos en el mundo del cumplimiento es una valiosa guía para miles de profesionales y estudiantes que empiezan su andadura en el camino del compliance corporativo. Entrevistamos a Miguel Ángel Jiménez-Velasco, un profesional con dilatada experiencia en la gestión del cumplimiento y en la actuali-

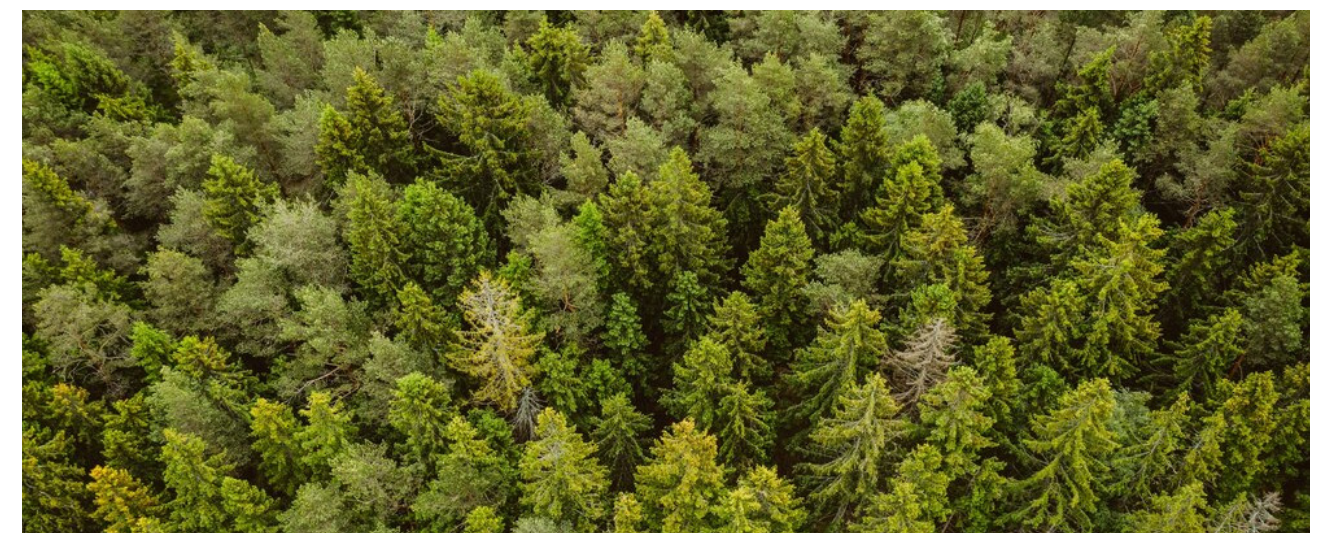
dad Director corporativo de cumplimiento del grupo Coxabengoa.

¿Nos podrías contar cuáles son tus principales funciones y responsabilidades en UN GRUPO como COXABENGOA, que actúa a nivel global y por lo tanto sometido a muy diversas legislaciones y jurisdicciones? ¿Cómo se gestiona un programa de cumplimiento a nivel mundial? ¿Qué características le infieren unidad?

Efectivamente, la nota concordante debe ser la unidad; la homogeneidad en los procesos y la uniformidad en las políticas. Un sistema de compliance a nivel consolidado puede ser vertical, piramidal, o transversal. Nuestro modelo es transversal, en el sentido de que cada vertical de negocio, cada geografía, cada jurisdicción local puede presentar particula-

ridades, bien para todo el modelo, bien para determinadas conductas o actividades, que deben ser analizadas e incorporadas al sistema. Ello sin perjuicio de la existencia de un core común para todo el grupo, empezando por el Canal de Denuncias y la Política de Prevención Penal. La seguridad de nuestro modelo radica en seleccionar siempre la norma más estricta e incorporarla para su aplicación a todo el grupo. Hay que estar muy encima de las distintas novedades legislativas y jurisprudenciales en las distintas jurisdicciones locales, y para ello son clave los equipos locales, tanto jurídicos como de cumplimiento.

En cuanto a las funciones dentro de un grupo internacional y con distintas líneas de negocio, lo fundamental es compartir una cultura común afín al cumplimiento, una voluntad de cumplir con la ley “más





allá de la letra de la norma"; la formación y la comunicación son actualmente más importantes incluso que una parametrización cuantitativa de los riesgos. El empleado con voluntad de cumplir debe inexorablemente conocer cuales son las actividades o acciones que debe evitar o consultar. No se trata tanto de vigilar como de supervisar.

¿Cuáles son los principales retos en materia de CUMPLIMIENTO a los que se enfrente el grupo?

En general el principal obstáculo del director de cumplimiento es siempre ganarse a la organización, y especialmente al órgano de administración y la alta dirección. Ser claro y transparente, constructivo, innovador en muchas ocasiones, conciliador, pero siempre predicando con el ejemplo y con las manos abiertas.

¿Cuáles han sido los mayores obstáculos y retos a los que tú te has enfrentado como oficial de Cumplimiento en una empresa con la historia y vicisitudes a las que se ha enfrentado Abengoa? ¿A qué retos se enfrenta un compliance officer en casos de crisis empresarial?

Abengoa siempre ha sido una escuela en todos los sentidos, para todos los empleados. El nivel de implicación profesional siempre fue muy exigente. En los más de treinta años en la compañía,

y habiendo estado al cargo de la secretaría general y del consejo, enfrentamos en 2010 el reto de, primero, entender esa novedad de que la persona jurídica pudiera delinquir, y, segundo, diseñar y aplicar un sistema "a ciegas" que cumpliera los requisitos apenas esbozados en el Código Penal. El proceso se culminó con la certificación UNE 19601 por parte de AENOR 2020-2023. Implantar, comunicar, convencer sobre ese cambio de paradigma penal no fue sencillo en un grupo a pleno funcionamiento. Por otra parte, durante la etapa preconcursal y de reestructuración, los riesgos relacionados con la solvencia pasaron a primer término, así como la protección de los administradores y directivos involucrados en el proceso, sin que hasta la fecha hayamos tenido nada en contra.

Lo mejor está siendo esta nueva etapa de integración con un grupo como Cox Energy, tan afín en cuanto a actividades y ambición. Y ello en ambos sentidos; estamos aprendiendo mucho del nuevo equipo de gestión, pero a la vez tratamos de aportar al grupo Cox algunos aspec-

tos de nuestra experiencia, actividades y sistemas, y está funcionando. Hay una compenetración a todos los niveles, con total respeto al papel que como adjudicatario tiene Cox.

¿Cómo compatibilizar el deber de diligencia y el deber de lealtad?

Muy fácil; lealtad una, a la empresa, representada por su órgano de administración y dirección como órgano colegiado, y diligencia, toda, empezando por los administradores y directivos personas físicas. Temas como las operaciones vinculadas, los conflictos de interés, la separación de funciones, etc. deben estar previamente reglados para servir como ejemplo a toda la organización. El diálogo con el consejo de administración tiene que ser fluido, periódico, pero también, dadas las distintas competencias y funciones del consejo y de las comisiones, debe ser conciso, práctico, sin circunloquios.

¿Consideras adecuada la regulación española de los programas de prevención de delitos? ¿Qué deberíamos aprender de los modelos de prevención de delitos de otros países?

Bajo mi punto de vista, es insuficiente la regulación legal de un concepto que se articula como eximente/atenuante en el Código Penal. El artículo 31.bis "hace lo que puede" sentando unas bases mínimas de qué hay que entender por modelo de gestión y que mínimos debe contener. Afortunadamente, la jurisprudencia del Tribunal Supremo y la existencia de estándares internacionales y nacionales bajo las normas ISO y UNE han facilitado en gran medida el diseño y la verificación de los sistemas de cumplimiento. La UNE 19601 aporta el rigor y la exactitud en todo un compendio de, por una parte, requisitos formales que dotan de seguridad jurídica al modelo, y, de otra, requisitos materiales en cuanto a la metodología del análisis de riesgos, la ponderación, la efectividad de los controles e indicadores, etc. Podemos decir que los profesionales contamos con las guías necesarias para un buen diseño e implantación. Pero falta otro aspecto tremendamente importante; la validez de estos modelos en el foro judicial. Me refiero al momento procesal oportuno para la prueba de la eficacia del

modelo, y a la parte procesal obligada a la prueba, así como al papel procesal de la representación especial de la persona jurídica investigada. Entiendo que las resoluciones judiciales por llegar irán aclarando estos aspectos y completando el marco de actuación procesal, siempre complejo y sensible.

En relación a la legislación española, de lege ferenda ¿Sería oportuno regular un estatuto del oficial de cumplimiento?

Al hilo del punto anterior, en la medida en que hablamos de una función, la de cumplimiento, y de un sistema o modelo de gestión que, al fin y al cabo, no están regulados como obligatorios (aunque ninguno podamos imaginar de qué otra forma podría cumplirse con los requisitos para que opere la eximente penal), parecería que la respuesta sería negativa; no es necesario una regulación específica del oficial de cumplimiento. Pero este punto de vista, parecido al que en 2010 podíamos tener ante la novedad de la responsabilidad penal de la persona jurídica, decae por su propio peso. Es necesaria una regulación procesal criminal de la representación, actuación y defensa de la persona jurídica como investigada (por ejemplo abordando los requerimientos de información a una persona jurídica aún no citada como investigada, por un delito incluido en la lista del 31.bis y que en consecuencia, tarde o temprano será atribuido también a la persona jurídica, y la posible indefensión que plantea en relación al derecho de no declarar contra sí misma) y del papel del representante especial de la persona jurídica en relación con el representante orgánico de ésta. De la misma manera, desde el punto de vista interno de la persona jurídica, se hace necesario una definición legal de la independencia y autonomía del oficial de cumplimiento, de su función e interacción dentro de la organización, del secreto profesional, y, sobre todo, del régimen de responsabilidad penal individual que puede llegar a tener dado su rol de responsable de cumplimiento de la compañía. Personalmente me decanto por la conveniencia, más que por la necesidad, de dotar a la función con un estatuto propio.

¿Cómo han evolucionado las políticas de anticorrupción de las compañías españolas en la última década? ¿se pueden entender homologadas a la de los países más avanzados en la lucha contra la corrupción?

Bajo mi punto de vista, en cuanto a políticas se refiere la evolución ha sido óptima. Pero la realidad del cumplimiento no



opera tanto en cuanto a políticas como en cuanto a los controles y supervisión. Debemos asegurar que la compañía cuenta con mecanismos internos de control que potencialmente pueden evitar o dificultar la comisión de una conducta no deseada. Hay que entender que no todas las empresas tienen la misma dimensión y por tanto los mismos recursos (en otras legislaciones las normas relativas a la responsabilidad penal de la persona jurídica operan solo a partir de una cierta dimensión, en términos de número de empleados, volumen de ventas etc.). De ahí la acertada definición de la función de cumplimiento como aquella que implementa un modelo de gestión.

De lo que se trata es de completar el sistema de gestión de una compañía, a todos los niveles de decisión, con los procedimientos y controles oportunos y eficaces, más que de elaborar políticas y códigos cuyo seguimiento es nulo. En este sentido, y desde las grandes compañías, financieras, energéticas etc., se agradece el efecto cascada de exigirnos a las más modestas que actuamos como proveedores o contratistas, requisitos de compliance que aquellas aplican. Por último, la involucración de los administradores y la alta dirección, el tone of y from the top, es imprescindible para extender la cultura de cumplimiento, el "behavioral compliance", desde el primero al último de los empleados.

No queriendo abusar de tu tiempo, una

última pregunta ¿Cuáles dirías que son los principales retos a los que deben hacer frente las empresas españolas en materia de compliance?

Desde el punto de vista doméstico, nacional, creo que estamos evolucionando favorablemente. No obstante, en algunos sectores, como en el mundo deportivo, la efectividad de la función de cumplimiento está enormemente condicionada por los grupos de poder. El esfuerzo que están haciendo los profesionales del compliance deportivo es digno de halago, y podría ser recomendable un mayor apoyo por parte de las administraciones, incluso a nivel regulatorio positivo.

Desde el punto de vista internacional, volviendo a lo que decíamos al principio, el reto es mantener la homogeneidad de un sistema propio de cumplimiento no ya en distintas líneas de negocio o geografías, sino en culturas distintas. El reto es entender y asimilar otras culturas distintas a la nuestra, en cuanto a la comunicación y formación, en las que no hay que vencer, sino convencer.

Muchísimas gracias, Miguel Ángel. Desde luego nos has apuntado cuestiones de máximo interés para la resolución, desde tu amplia experiencia, de los retos a que se enfrenta la gestión de compliance y su regulación. Desde las páginas de "European Compliance & News" te agradecemos tu generosa aportación y te deseamos los mayores éxitos profesionales.



coxabengoa
evolución natural

IA Y LOS DERECHOS HUMANOS EN EL MUNDO DEL TRANSHUMANISMO



Manuel Lázaro Pulido

Catedrático. IP. Grupo de Investigación "Iure hominis.

Derechos Humanos: fundamentación y protección jurídico-política" (UNIR)

Universidad Internacional de La Rioja.

La irrupción de la inteligencia artificial (IA, en inglés AI) es un fenómeno que ha inundado el lenguaje usado en los diversos contextos semánticos de la vida social tanto formales (academia, mundo empresarial, discursos políticos...) como informales (el lenguaje de la calle, de las personas en su vida cotidiana, especialmente en realidades disruptivas como el Chat GPT, nacido en 2018 y llevado al estrellato en su versión GPT-4 lanzado por OpenAI). La inclusión de las siglas IA no pueden olvidar su entorno más amplio: el entorno digital, el espacio donde la IA trabaja con los Big Data.

Cada vez que existe un avance en la humanidad, este plantea problemas éticos que nos lleva a preguntarnos por el impacto que sobre nuestra vida como seres humanos tiene la implementación de estos nuevos productos diseñados y realizados por el hombre. La IA no es ajena a esa cuestión, pero a diferencia de otras realidades, esta se ha enmarcado dentro de un nuevo fenómeno antropológico que precisamente tiene en la propia IA su motor de transformación. No solo se trata de que algo novedoso plantea retos éticos, sino que el nuevo reto, en este caso tecnológico, impulsa a no pocos actores intelectuales a redefinir la propia noción del ser humano y, no pocas veces, se presenta en cierta forma al gran público como un fenómeno que tiene una existencia casi paralela a la propia del hombre.

Si hablamos de IA es porque las tecnologías que se basan en ella están cada vez más presentes en la vida de todos, a través, por ejemplo, de la domótica o las redes sociales, y son usadas por dife-



rentes instancias privadas y también públicas para cuestiones que tienen que ver con el uso instrumental en y para las actividades cotidianas, sino para penetrar en la intimidad humana, por ejemplo, evaluando la personalidad o las aptitudes de las personas, asignando recursos o protagonizando las tomas de decisiones. No escapa a nadie que estas realizaciones de la IA pueden tener consecuencias graves y concretas para los derechos humanos. Ante esta circunstancia se plantean diferentes y graves cuestiones que precisan de una normativa que sea capaz de responder a estos retos y el compromiso de las instituciones públicas, las organizaciones civiles y las empresas de un cumplimiento identificable, rastreable y efecti-

vo de estas normativas.

Sobre este tema ya se reflexiona desde diversas perspectivas. Pero lo que aquí queremos señalar es el contexto ético y antropológico que está detrás del fenómeno o, al menos, que se presenta de forma concomitante y que afecta a la relación con el núcleo ético-normativo fundamental del mundo occidental y que tiene un soporte con vocación universal: los derechos humanos. Es decir, la cuestión que se presenta en la relación entre IA como un fenómeno que parece que traspasa la propia dimensión instrumental y que afecta la propia percepción que el hombre tiene de sí mismo y el horizonte ético normativo de unos derechos del hombre, digamos tradicional.

Estos dos planos de reflexión entre IA y derechos humanos (perspectiva instrumental de la IA y antropológica) tienen como trasfondo la misma mirada que demos a la IA: de forma más restringida (estrecha) o de manera más amplia (general). Cada punto de vista plantea una reflexión de la relación entre IA y derechos humanos, y estos puntos de vista no son exclusivos, sino que para muchos representan estadios diferentes del desarrollo de la IA

PENSAR LOS IA Y DERECHOS HUMANOS DESDE LA INTELIGENCIA ARTIFICIAL ESTRECHA (IAE) EN UN CONTEXTO HUMANO: LAS INSTANCIAS INTERNACIONALES

Definir la IA

Cada realidad se entiende en su definición, en su delimitación. Cada definición designa referencialmente una realidad, por lo que definir de forma diferente una expresión implica entender la realidad que soporta el concepto que conlleva dicha expresión de modo distinto. Este hecho cognitivo, lingüístico y ontológico se deja ver también en la definición de la IA. Desde que John McCarthy, considerado el padre de la IA, definió en la conferencia de Dartmouthen, en 1956, la IA como "la ciencia e ingeniería para fabricar máquinas inteligentes", su desarrollo en las distintas olas de implementación desde sus primeros pasos (1950-1979), su evolución (1980-2000), pasando por la edad de oro (2010-2019), hasta llegar a la era actual (2020-), así como sus implicaciones, han ido reformulando esta definición haciendo compleja la adopción de un criterio unánime. Las definiciones se han multiplicado y en no pocas regulaciones se tiene que optar por una definición consensuada como punto de partida. La definición de la IA está en relación con su desarrollo, y, como hemos señalado antes, las diferentes perspectivas responden en parte sustancial a diferentes etapas de desarrollo. Así hablamos de una Inteligencia Artificial Estrecha – IAE (*Artificial Narrow Intelligence* – ANI), de una Inteligencia Artificial General – IAG (*Artificial General Intelligence* – AGI) y, algunos hablan de un desarrollo hiper, en tanto que Super Inteligencia Artificial – SIA (*Artificial Super Intelligence*–ASI).

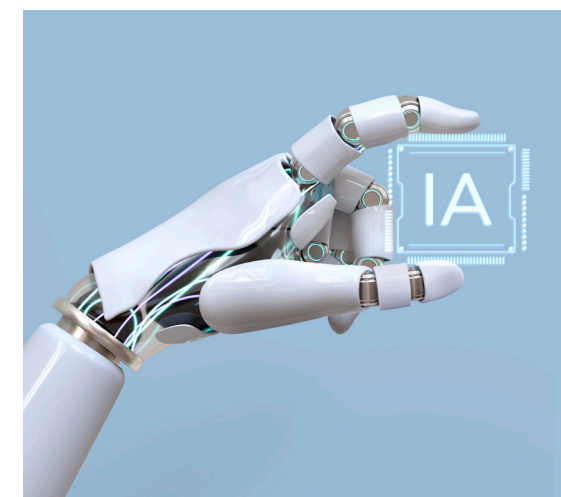
La IAE es la categoría más elemental y conocida, se trata de una IA que no es capaz de superar a los humanos. Podemos decir que todos los programas y herramientas que utilizan IA hoy en día, incluso los más avanzados y complejos, son formas de IAE. Y estos sistemas es-

tán por todas partes. Los smartphones están llenos de aplicaciones que utilizan esta tecnología, desde mapas GPS que te ayudan a orientarte por el mundo o a conocer el tiempo, hasta programas de música y vídeo que conocen tus gustos y te hacen recomendaciones. Los asistentes virtuales como Siri y Alexa, el motor de búsqueda de Google y el robot que limpia la casa también son formas de IAE. Incluso los sistemas más sofisticados, como los coches sin conductor (o vehículos autónomos) y los populares ChatGPT, son formas de IAE, porque no pueden operar fuera del rango predefinido por sus programadores, y, por tanto, no pueden tomar decisiones por sí mismos.

La preocupación de IAE se centra en aceptar y aprovechar la idea de que los humanos y las computadoras tienen diferentes fortalezas y competencias relativas. La IAE se inscribe en una visión de máximos utópica, dentro del horizonte de la definición de ser humano. En este sentido la IAE desarrolla sus fortalezas dentro de la rapidez y eficiencia en la ejecución de tareas cognitivas, es decir, en el desarrollo de reglas lógicas y explícitas. Los sistemas IAE suelen entrenarse utilizando un amplio conjunto de datos (por ejemplo, de Internet) y pueden tomar decisiones o emprender acciones basándose en este entrenamiento. En este sentido, puede igualar o superar la inteligencia y eficacia humanas, pero solo en el ámbito específico en el que opera. El ejemplo –que ya es clásico– es el de los programas de ajedrez que utilizan IAE, capaces de vencer al campeón del mundo en esta disciplina, pero no pueden realizar otras tareas.

La vertiginosa gestión de datos y problemas enclaustrados, que ya es de por sí llamativa, impide a la tecnología IAE carecer de autoconciencia, una característica muy significativa de la inteligencia humana. Su mirada escapa a las capacidades eficientes en los humanos tales como la gestión de situaciones ambiguas o aquellas que requieren intuición, creatividad, emoción, juicio y empatía. La IAE tiene una inteligencia más rápida, pero no más completa. En este sentido, desarrolla áreas de procesamiento de datos tales como la visión artificial, el procesamiento del lenguaje natural (PLN), el reconocimiento de sonidos vocales, los sistemas basados en el conocimiento y la planeación automatizada entre otras tareas.

Esta tecnología desafía los derechos humanos en sí, en el uso de sus aplica-



ciones, y también en la proyección que tienen para desarrollar distintas etapas que afectan a la tecnología, pero, sobre todo, a la visión y proyección a los que apunta: IAG y SIA, respectivamente.

Ante estos retos tan importantes para el desarrollo del ser humano en un contexto de defensa de los derechos humanos, cabe entender que, a principios de 2023, más de 350 líderes de IA firmaron una declaración en la que instaban a la comunidad internacional a dar prioridad a la mitigación del riesgo de "extinción" que plantea la IA, poniéndolo al mismo nivel que una pandemia o una guerra nuclear. Un riesgo que nace no solo por lo que IAE hace o puede hacer. Sirva de ejemplo su uso en el sector de los servicios financieros tales como la evaluación de riesgo en el préstamo y la proyección de inversiones en un terreno de volatilidad volitiva (mentalidad de rebaño) como es el financiero. Es un ejemplo que se puede derivar en su proyección en el área de la política. A los riesgos de las aplicaciones concretas se le suma el déficit de transparencia. Pero esto que es en sí preocupante no es lo único, aunque quizás sea lo más visible. Quizás lo más preocupante, y lo más olvidado, es la creación de una mentalidad antropológica distorsionada que diluye –sustituyéndola– la utopía humana en una distopía transhumana.

Desde la realidad de la IAE existen respuestas a nivel de organismos internacionales de las relaciones existentes entre esta y los derechos humanos es el caso del Consejo de Europa y de las Naciones Unidas.

EL CONSEJO DE EUROPA

El Consejo de Europa es nuestro contexto político y normativo general más cercano. El 9 de diciembre de 2023 se publicó en comunicado de prensa que

se había “alcanzado un acuerdo provisional sobre la propuesta relativa a normas armonizadas en materia de inteligencia artificial (IA), el denominado «Reglamento de Inteligencia Artificial»”. Como señala el propio comunicado su objeto es garantizar que los sistemas de inteligencia artificial (IA) introducidos en el mercado europeo y utilizados en la UE sean seguros y respeten los derechos fundamentales y los valores de la UE. Se sigue señalando que los principales nuevos elementos del acuerdo provisional pueden resumirse en:

- Normas sobre modelos de IA de uso general de gran impacto que pueden causar un riesgo sistémico en el futuro, así como sobre los sistemas de IA de alto riesgo;
- Un sistema revisado de gobernanza con algunas competencias de ejecución a escala de la UE;
- Ampliación de la lista de prohibiciones, pero con la posibilidad de utilizar la identificación biométrica remota por parte de las autoridades policiales en espacios públicos, con sujeción a salvaguardias;
- Una mejor protección de los derechos mediante la obligación de que los implementadores de sistemas de IA de alto riesgo lleven a cabo una evaluación del impacto en los derechos fundamentales antes de poner en marcha un sistema de IA.

En relación con los derechos fundamentales, se exige su transparencia y protección. Para ello se propone una evaluación del impacto y un refuerzo de la transparencia en los derechos fundamentales antes de que un sistema de IA de alto riesgo sea introducido en el mercado por sus implementadores. Se insiste en la obligación de los usuarios de un sistema de reconocimiento de emociones de informar a las personas físicas a las que se exponga a un sistema de este tipo.

El horizonte del documento centrado en el respeto y protección de los derechos fundamentales tiene como marco la Agencia de los Derechos Fundamentales de la Unión Europea. La FRA (European Union Agency for Fundamental Rights) publicó, en 2021, el documento *Construir correctamente el futuro. La Inteligencia Artificial y los Derechos Fundamentales* que tiene como marco global la Carta de los Derechos Fundamentales

de la Unión Europea, así como de la Convención Europea de Derechos humanos. El documento analiza las principales consecuencias, tanto positivas como negativas, para los derechos fundamentales de las nuevas tecnologías, incluida la IA en cuatro ámbitos clave: prestaciones sociales, policía predictiva, servicios sanitarios y publicidad selectiva, centrandose el análisis en la responsabilidad empresarial y administrativa para con el ciudadano y el derecho que las personas tienen a saber que se ha utilizado la IA, y al tiempo y forma en que pueden presentar una reclamación.

Pero su raíz es más profunda en el tiempo y en la base. Se trata de un último peldaño en la toma de conciencia que las autoridades europeas han tomado sobre los desafíos que los efectos de los sistemas de IA plantean a los derechos fundamentales y, por lo tanto, a los derechos humanos. Ya el 14 de mayo de 2019 la Comisión publicó la Recomendación *Unboxing artificial intelligence: 10 steps to protect human rights (Descifrar la inteligencia artificial: 10 medidas para proteger los derechos humanos)*. Este documento tenía un cariz más fundamental respecto del significado de la IA respecto de los derechos humanos. De hecho, el documento está firmado por la Comisaria de derechos humanos y en su redacción colaboraron Nani Jansen Reventlow, abogada especialista en derechos humanos y Directora de Digital Freedom Fund, y Jonathan McCully consultor independiente y también asesor jurídico de Digital Freedom Fund.

El documento reconoce que “los efectos de la inteligencia artificial (IA) sobre los derechos humanos es uno de los factores más importantes que definirán el periodo en el que vivimos”. Ante la divergencia conceptual, su posición desarrollada, en cierta forma, la definición propuesta por la OCDE, en 2018 (“la disciplina de crear algoritmos con la capacidad de aprender y razonar”) y propone una definición general, descriptiva, pero a la vez menos instrumental y más relacionada con las capacidades por lo que ya en sí resulta interesante. La IA se define como “una expresión genérica utilizada para designar de manera general un conjunto de ciencias, teorías y técnicas cuyo objetivo es mejorar la capacidad de las máquinas para realizar tareas que requieren facultades cognitivas”.

Ante el desafío que ello conlleva se proponen una serie de medidas para que las autoridades nacionales aprovechen al máximo el potencial de los sistemas de

inteligencia artificial y, al mismo tiempo, eviten o mitiguen sus efectos negativos en la vida y los derechos de las personas. se centra en 10 ámbitos principales de actuación:

- Evaluación del impacto en los derechos humanos.
- Consultas públicas.
- Normas de derechos humanos en el sector privado.
- Información y transparencia.
- Supervisión independiente.
- No discriminación e igualdad.
- Protección de datos y privacidad.
- Libertad de expresión, reunión y asociación, y derecho al trabajo.
- Oportunidades de reparación.
- Fomento del conocimiento y la comprensión de la inteligencia artificial.

Si nos fijamos, el primer y el tercer punto señalan de forma directa el tema de los derechos humanos, si bien los otros apartados se relacionan transversalmente con ellos. Aquí no se mencionan los derechos fundamentales que, como sabemos, no se equiparan de forma simbiótica con los derechos humanos. Se habla directamente de la evaluación del impacto sobre los derechos humanos, de modo que el horizonte en el que los Estados miembros deben aplicar medidas adicionales frente a los agentes de la IA es el respeto de los derechos



humanos que alimentan los derechos fundamentales. En este sentido, esta primera aproximación revelaba un horizonte semántico que excedía el terreno jurídico-normativo propio de los derechos fundamentales.

En 2023, la Comisaria de los derechos humanos del Consejo de Europa, bajo el asesoramiento de los dos mismos expertos, publica la Recomendación de seguimiento al documento anterior: *Human rights by design future-proofing human rights protection in the era of AI*. Con un contenido de siete capítulos (menos que el anterior) intenta ofrecer unas orientaciones con el fin de garantizar la protección de los derechos humanos en la era de la inteligencia artificial, integrando la cuestión de los derechos humanos en el diseño de los sistemas de IA (IAE). Se recuerda que los Estados miembros deben, por ejemplo, evaluar los riesgos y las consecuencias de los sistemas de IA para los derechos humanos antes de utilizarlos, reforzar las garantías de transparencia y garantizar la supervisión independiente y el acceso a recursos efectivos. Una idea que realmente es interesante y real es que se debe desterrar la idea (o el mito) de que la IA es tan compleja y misteriosa que escapa al control humano y, que por lo tanto no existe posibilidad de una regulación eficaz.

En relación con los derechos humanos se señala, en primer lugar, la necesidad de afrontar el tema de forma global y no sectorial, es decir, simplemente teniendo en cuenta subconjuntos de derechos particulares. Se subraya la necesidad del incremento de transparencia e intercambio de información, así como afianzar las iniciativas de los Estados miembros para utilizar la IA con el fin de reforzar los derechos humanos. El diseño, desarrollo y despliegue de los sistemas de IA no pueden vivir ajenos a los derechos humanos y los Estados miembros deben proteger la supervisión y el control, señala la Comisaria Dunja Mijatović. Ante esta situación el Consejo de Europa ha terminado creando el Comité sobre Inteligencia Artificial (CAI), presidida por el suizo Thomas Scheider, que es el resultado de un proceso iniciado en 2018 en el Consejo de Europa sobre el tema específico de la IA, que ya en su 4ª sesión plenaria (2 de marzo de 2023), decidió hacer público el “Borrador Cero” revisado de la Convención [Marco] sobre Inteligencia Artificial, Derechos Humanos, Democracia y Estado de Derecho.

NACIONES UNIDAS

La conciencia europea está en sintonía con las reflexiones realizadas en el seno de Naciones Unidas, consciente de que estamos en el umbral de una nueva era. La directora general de la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO), Audrey Azoulay afirmaba que “la IA es la nueva frontera de la humanidad” (“Towards an Ethics of Artificial Intelligence”, December 2018, Nos. 3 & 4 Vol. LV, “New Technologies: Where To?”). Planteaba las diferentes etapas de la IA, pero a diferencia del Consejo de Europa que se situaba en un horizonte de principios de IAE, centrándose en la forma de gestión de la herramienta, aquí se plantea una cuestión antropológica y de civilización:

“Una vez cruzada, surgirá una nueva forma de civilización humana. El principio rector de la IA no es convertirse en autónoma ni sustituir a la inteligencia humana. Pero debemos asegurarnos de que se desarrolle de forma humanista, basada en valores y derechos humanos. Nos enfrentamos a una cuestión crucial: ¿qué tipo de sociedad queremos para el mañana? La revolución de la IA abre nuevas y apasionantes perspectivas, pero las conmociones antropológicas y sociales que está provocando merecen una atenta reflexión”.

Aun así, Naciones Unidas, lógicamente en lógica IAE, se centra en el horizonte de la gestión: los riesgos del uso malintencionado, el servicio al bien común... y, ¡cómo no! crear una nueva estructura en la ONU, tal como avanzó el secretario general António Guterres el 18 de julio de 2023. En 2021 el Alto Comisionado de las Naciones Unidas para los Derechos Humanos, Michelle Bachelet apelaba que el mundo actuara de inmediato ante la “escala colosal” de violaciones de derechos del hombre que podría suponer la IA.

Los derechos humanos –afirma Volker Türk, Alto Comisionado de las Naciones Unidas para los Derechos Humanos– deben ser el ancla que sujete la investigación en IA: “El marco de los derechos humanos proporciona una base fundamental la cual puede facilitar protecciones a la hora de emplear esfuerzos para explotar el enorme potencial de la IA, a la vez que se previenen y mitigan sus enormes riesgos implícitos” (Declaración del 12 de julio de 2023). Dos días más tarde, el Consejo de Derechos Humanos de la ONU adoptó una resolución que insta a la comunidad internacional a tomar medidas para proteger y supervisar la IA. La resolución

pide promover la “transparencia” de los sistemas de IA y garantizar que los datos de esta tecnología “se recopilan, utilizan, comparten, archivan y eliminan” de forma compatible con los derechos humanos. La UNESCO, por su parte, prepara para los días 5 y 6 de febrero de 2024 el segundo Foro mundial sobre la ética de la inteligencia artificial centrado en la gobernanza de la IA que desarrolla el documento *Recomendación sobre la ética de la inteligencia artificial*, adoptada el 23 de noviembre de 2021 por los 193 estados miembros de UNESCO y que constituía el primer instrumento normativo mundial sobre la IA. La Recomendación tiene como piedra angular la protección de los derechos humanos y la dignidad, basada en la consolidación de principios fundamentales como la transparencia y la equidad, sin perder nunca de vista la importancia de la responsabilidad humana en el control de los sistemas de inteligencia artificial.

PENSAR LOS IA Y DERECHOS HUMANOS DESDE LA INTELIGENCIA ARTIFICIAL GENERAL (IAG) EN UN CONTEXTO TRANSHUMANO: LOS RETOS DEL PENSAR

Pero la pregunta que nos hacemos aquí tiene en cuenta el futuro próximo de la IA: ¿nos dirigimos hacia la IAG, Inteligencia artificial general? La IAG representa, señalan algunos especialistas del mundo tecnológico, el Santo Grial de la IA. Se trata de un horizonte que visualiza un sistema inteligente capaz de razonar, aprender y crear de forma autónoma y multifuncional, acercándose a la versatilidad y flexibilidad de la inteligencia humana. Mientras el mundo se adapta al impacto de la GPT-4, el futuro de la IA mira ya más lejos con el anuncio de la GPT-5, una incipiente grieta hacia la IAG. Esta implica que una máquina adquiere capacidades cognitivas de nivel humano, es decir, que tiene la capacidad de realizar cualquier tarea intelectual que pueda realizar una persona. AGI es un campo emergente. Y si IAE muestra retos fundamentales en el campo ético y normativo, lo avances en IAG vienen acompañados no solo de importantes cuestiones éticas y retos de seguridad y gobernanza, sino de cuestiones antropológicas que nos hace navegar entre la utopía y la distopía en la era de la IA.

Efectivamente, por una parte IAE e IAG nos marcan un horizonte utópico en cuanto que su propio relato nos muestra avances deslumbrantes e interrogantes constantemente renovados, dirigién-

donos hacia una utopía tecnológica que refuerza el cumplimiento de los derechos humanos y fundamentales: sistemas de protección de la vida privada, asistencia a personas con discapacidad, mejora en los sistemas de información, aplicación a la justicia penal, control de las falsas noticias (*fake news*), y yendo más a la IAG, enfermedades curadas gracias a diagnósticos médicos avanzados, desastres medioambientales evitados gracias a una gestión optimizada de los recursos, e incluso la eliminación de la pobreza mediante sistemas económicos inteligentes.

Pero aparece en el horizonte un panorama también distópico que no solo afecta a un posible descontrol de la IA, o a su utilización descontrolada, sino a la propia definición humana y, por lo tanto, de los derechos humanos, en tanto que se pone en cuestión la naturaleza humana

En enero de 2018 Chia-Rong Tsao escribió un trabajo titulado "A Posthumanist Reflection on the Digital Humanities and Social Sciences" (dentro del libro *Big Data in Computational Social Science and Humanities* (Springer) pp. 365-377). En él se realizaba una aproximación a la implicación de la epistemología de la IA y la tecnología digital desde la perspectiva teórica "posthumanista". Según esta perspectiva, que tal como lo formula podría llamarse quizás mejor "transhumanista", las tecnologías digitales afectan inevitablemente a las prácticas de investigación y a la producción de conocimientos actuales y, lo que es más importante, los investigadores también experimentan transformaciones fundamentales en este proceso de "co-constitución" (p. 366). Se trataría de una perspectiva posthumanista en el que se subraya la interacción entre humanos y máquinas, en una apuesta casi distópica, en la que lo posthumano es un organismo cibernético que supone, desde esta perspectiva, una crisis del sujeto moderno, en la medida en que no se visualiza bien las fronteras entre lo humano y lo no humano (IAG).

Esta perspectiva es atractiva, en el sentido que juega en la frontera de la ciencia ficción, esto es, proyecta en un futuro –cibernético y no realizado–, un deseo presente: el de crear la sensación de la "debilidad" humana. No obstante, la atracción de la propuesta nace de la propia desazón que provoca en el lector, una inquietud que no beneficia en nada a la IA y que la desvía de su intrínseca esencia: un desarrollo realizado por seres humanos para estudiar, analizar y crear

productos "humanos".

Vivimos con frecuencia abocados a la imagen del dilema de la Esfinge que narrara Apolodoro, primero y reprodujera Diodoro Sículo y Aristófanes después: "¿Qué ser provisto de voz es de cuatro patas, de dos y de tres?". La respuesta, recordemos, nos habla de una imagen del hombre que, de niño, anda a "cuatro patas", siendo adulto deambula "con dos" y en la senectud se apoya con el bastón, por lo que camina con "tres patas". Esta respuesta biológica esconde otra profunda mirada desde la perspectiva de la historia cultural. La de un hombre mitológico representado por las cuatro patas y la del hombre prometeico, dotado de inteligencia, de logos, que realiza su vida cultural mediante dos patas, erguido, con la cabeza mirando al frente, en perspectiva y capaz de elevar sus ojos hacia las alturas. Por último, la del ser humano que desarrolla su ser apoyándose en una herramienta, en un artilugio, hoy en la tecnología, la IA. La cuestión es: ¿esa herramienta –representada por el bastón– es una herramienta que impulsa al hombre a ir más allá y mejor en el deambular de su vida, en su camino por el tiempo y el espacio, o es un elemento que transforma su propia naturaleza, reformulando su inicial estado mitológico, hacia otra naturaleza que le sobrepasa, reviviendo la mitología desde el posthumanismo, convertido ahora en un ciborg (una criatura posthumana)?

No obstante, los que lean esta reflexión, no se asusten. Seguimos en el horizonte de IAE. Estamos aún alejados de las distópicas ensoñaciones de Skynet en *Terminator*, o de la emotividad asesina del mítico ordenador HAL 9000 de la película *2001 Una Odisea en el Espacio* o la más calmada de *Inteligencia Artificial* de Steven Spielberg. No se trata de la afectividad cuasi humana de los replicantes de *Blade Runner*, ni siquiera nos encontramos en el mundo de *The Matrix*, una simulación de una SIA (el horizonte distópico de IA). La amenaza de Matrix no reside en la matriz, ni en los Big-Data, ni en IA, ni en los ciborgs. El peligro descansa en el uso que los seres humanos pueden hacer y hacen del entorno digital y la IA cuando son "demasiado humanos". No descuidarse en proyecciones ficticias es necesario para poder analizar el presente. Se trata de no caer en las distracciones del ilusionista. El problema no está en el transhumanismo, sino en olvidar el humanismo que deben guiar los pasos del quehacer humano. Eso es lo que toca.

En este sentido, IA se presenta al ser humano con etiologías diversas, que con frecuencia responden a intereses espurios (que también son humanos e, incluso, son muy humanos). Se trata de optimizarlos en un contexto de responsabilidad humana y social. La era de la IA y el "Big Data" implica, sin duda, la aparición de nuevos paradigmas de generación, recolección y almacenamiento de grandes volúmenes de datos en formato diverso. Puede ser una oportunidad de desarrollo de lo humano, y solo así de los derechos humanos, un espacio de humanización en tanto que, siendo elementos imprescindibles para el análisis de nuestro quehacer humanístico, son empleados como instrumentos de observación humana. No será la primera vez que tecnologías creadas para usos potencialmente peligrosos para el hombre o como resultado del miedo humano, de la defensa, de la tecnología para uso militar, se convierten en elementos de uso civil. Pero tampoco será la primera vez que el uso civil, desprovisto de un humanismo consciente, termina siendo más peligroso aún que su origen militar, si este ha estado transido de un elemento ético.

En este sentido resulta más útil, considerar la IA desde una reflexión filosófica (racional, axiomática, ética...) relativa a la propia cultura digital en el entorno vital y existencial humano. Efectivamente, uno de los retos del siglo actual se plantea en los términos acerca de la influencia que los nuevos soportes y herramientas de producción cognitiva (IAE) tienen en la cultura, en la sociedad, en el acceso cultural y en la propia definición de realidad humana. Más aún, en cuanto cuestionamiento en sí, en la filosofía, lo que ha provocado un pensamiento sobre la interacción renovada entre ciencias, tecnologías y culturas. Detrás de las tecnologías computacionales y digitales existe todo un contexto de racionalidad, proyectos humanos y culturales, representación y recreación del mundo... que desafía la propia lógica digital, toda vez que esta no deja de ser desarrollada por seres humanos. Y este horizonte humano debe ser el motor de la IA y el universo digital, la guía que nos debe hacer sentir miembros de este proyecto, el acicate para poder defender los derechos humanos y no desviarnos hacia un horizonte transhumano que distorsiona la proyección ilusionada de la utopía en un espacio de distopía. El motor que alimenta la responsabilidad humana y social (compliance) de cada uno de nosotros y de las instituciones públicas y privadas que hemos construido.

COMPLIANCE Y SUBROGACIÓN LABORAL



Belén Luzuriaga
Directora de cumplimiento.



Cuando hablamos de Cumplimiento, sin duda, el elemento clave son las personas. Son las que hacen que en cualquier centro de trabajo se respire una cierta cultura de cumplimiento, que es la que se conforma con los valores y los principios que en una organización se consideran fundamentales. De ahí, la relevancia de que los códigos éticos o de conducta no se limiten a ser mero papel.

Y cuando hablamos de subrogación laboral, también hablamos de personas, porque son las personas trabajadoras las principales destinatarias de esta figura legal que les permite continuar prestando sus servicios en un centro de trabajo con independencia de la empre-

sa que resulte adjudicataria del servicio al cual están adscritas.

Por lo tanto, la ecuación de Compliance y de Subrogación pasa necesariamente por tener en cuenta a las personas. Las empresas necesitan profesionales para llevar a efecto su objeto y, en nuestro país, la existencia de la obligación de subrogar al personal que se contempla en varios sectores de actividad pone en evidencia una serie de prácticas que "quizá" no sean del todo compatibles con el Cumplimiento.

Si nos referimos a contratos públicos, es sabido que las normas administrativas tienen una loable intención: que resulte

adjudicataria la empresa con la oferta económicamente más ventajosa, que es la que se valora como de mejor relación calidad-precio, que no tiene que ser necesariamente la más barata. Pero queda en eso, en intención, dado que las propias normas permiten ser sorteadas con éxito y que existan verdaderas subastas revestidas de "Cumplimiento" por parte de los organismos licitadores.

En cuanto a la contratación entre empresas privadas, donde el precio es el que impera, podría buscarse la calidad del servicio, pero realmente, esto es algo accesorio para los departamentos de compras en la mayoría de las ocasiones, puesto que su interés se centra en cum-



plir con sus indicadores que, por lo general, suelen ser meramente económicos.

Lo que queda en evidencia es que cada protagonista piensa exclusivamente en sí mismo, el organismo contratante, ya sea público o privado, en pagar lo menos posible por el servicio que contrata; la empresa que realiza el servicio, en rentabilizar el contrato del cual ha resultado adjudicataria; y, las personas trabajadoras, en que su nueva contratadora sea una empresa que pague sus nóminas cada mes. A esto se reduce todo, ¡así de simple!

Y mientras tanto, por el camino nos olvidamos que existen obligaciones para cada uno de estos actores y que es preciso que se cumplan si realmente queremos empezar a hablar de Cumplimiento.

Entre esas normas encontramos la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014, que regula la obligación de subrogación laboral en los contratos del sector público en el

artículo 130, cuando una norma legal, un convenio colectivo o un acuerdo de negociación colectiva de eficacia general, imponga al adjudicatario la obligación de subrogarse como empleador.

La LCSP obliga a los servicios dependientes del órgano de contratación a facilitar a los licitadores, en el propio pliego, la información sobre las condiciones de los contratos de los trabajadores a los que afecte la subrogación, de cara a practicar una exacta evaluación de los costes laborales. Esa información es la que la empresa que viniese efectuando la prestación objeto del contrato a adjudicar, y que tenga la condición de empleadora de los trabajadores afectados, está obligada a proporcionar: listados del personal objeto de subrogación, el convenio colectivo de aplicación, detalles de categoría, tipo de contrato, jornada, fecha de antigüedad, vencimiento del contrato, salario bruto anual de cada trabajador, así como todos los pactos en vigor aplicables a los trabajadores a los que afecte la subrogación.

Con esos datos aportados en el pliego, las empresas hacen sus propuestas, sabiendo que las reglas de juego, admitidas por todos, contemplan la posibilidad cierta del “engaño”. Aquí es donde deben entrar los órganos de Competencia, que necesariamente deberían multiplicarse si se pretende conseguir el Cumplimiento Normativo en las licitaciones.

Me pregunto qué pasaría si todas las administraciones fueran capaces de gestionar eso que se llama coordinación de actividades empresariales, que es una obligación legal básica para la prevención de riesgos laborales..., nada raro, todas las empresas saben lo que deben hacer, pero ya se sabe, si el cliente no solicita nada, ¡mejor! Menos trabajo. Si cada responsable de un servicio fuera consciente de la responsabilidad que conlleva esa gestión, seguramente trataría por todos los medios de que existiera la gestión del CAE. A propósito, ¿Para cuándo la obligación de un Compliance en todas las entidades del sector público? ¿Por qué no es una obligación legal disponer de un programa de prevención de delitos para contratar con las administraciones?

Vamos al grano, la gestión del CAE permitiría a las entidades del sector público disponer en tiempo real y de forma fiable de toda esa información que se debe poner a la hora de redactar un pliego de licitación, sin depender de la “creatividad” empresarial para el traslado de esos datos. Si las administraciones

comienzan por cumplir su obligación de gestión del CAE, se podría empezar a pensar en un Cumplimiento real por parte de los actores involucrados en la cadena de contratación. Ya se sabe: lo que mal empieza...

Porque la paradoja es que la administración simplemente comunicará al nuevo empresario la información que le ha sido facilitada por el anterior contratista, es decir, no es responsable de la veracidad de los datos aportados en el pliego, llegando a exponer la LSCP que en el caso de que una vez producida la subrogación si los costes laborales fueran superiores a los que se desprendieran de la información facilitada por el antiguo contratista al órgano de contratación, el contratista tendrá acción directa contra el antiguo contratista. Es decir, la administración licitadora se lava las manos y queda el juego entre las empresas competidoras, que recordemos juegan con las mismas reglas y se engañan unas a otras de forma natural, ya que saben que unas veces se sale ganando y otras perdiendo, pero al final parece que a todas les compensa continuar olvidándose de eso que se llama Cumplimiento. Es decir, ¡no pasa nada! Pero, si la Administración fuese la responsable de la veracidad de esos datos que se trasladan en el pliego, ¡Podría empezar a pasar algo!

Se trata de voluntad de Cumplimiento en las licitaciones públicas y, aunque existen normas, no se están cumpliendo por parte de los actores intervinientes. Así perpetuamos un sistema que no se adecúa al Compliance. Debemos cambiar las reglas del juego para que realmente se cumplan y, de momento, ¿Seguimos permitiendo que se hagan trampas con el dinero de todos? Porque al final, no nos engañemos, se trata de dinero.

Se supone que la subrogación contribuye a que el mercado laboral sea mejor, permite asegurar un puesto de trabajo al personal y a las empresas disponer de profesionales de forma inmediata, con los pros y contras que eso conlleva. Pero, qué ocurre con los derechos adquiridos por las personas subrogadas, imaginemos un plan de igualdad, cada empresa dispone de su propio plan, si consideramos que esa subrogación se debe contemplar teniendo en cuenta todos los pactos, ¿Los derechos contemplados en un plan de igualdad podrían ser reclamados a la hora de subrogarse a otra empresa que no los contemple? Habría que preguntarse si tiene sentido una norma que obliga a las empresas a

disponer de plan de igualdad sin haber tenido en cuenta la existencia de la subrogación laboral obligatoria en varios sectores de actividad en nuestro país, como puede ser la limpieza. Es una incongruencia normativa legislar normas de forma aislada sin tener en cuenta el acervo legal existente. ¿Qué pasaría si alguna persona reclama continuar aplicando un plan de igualdad al ser subrogada a otra empresa? ¿Cumplir con la igualdad permitiría aplicar diferentes planes dentro de una misma empresa? ¿Cabe la posibilidad de que alguien reclame los derechos que se reconocen a su compañero subrogado?

Podemos abrir infinitas cuestiones: ¿Se respeta el tratamiento de los datos personales en las licitaciones con personal a subrogar? Podría haber la posibilidad de identificar el salario de determinadas personas que tuviesen una categoría específica en exclusiva en relación con el resto de personal... ¿Se aplican las normas de protección de datos cuando las empresas trasladan la información del personal ante una subrogación laboral? ¿Se incluye a las personas subrogadas en los planes de formación anuales de las empresas? ¿Existen los mismos permisos para el personal subrogado que para el personal de estructura no subrogable en las empresas?

Y, ¿Qué hay en la posibilidad de corrupción en los negocios en los contratos privados? ¿Se tienen en cuenta los programas de cumplimiento de cada empresa, los códigos éticos y los riesgos penales en la presentación de propuestas, negociación y contratación? ¿Cuántas empresas están trabajando ya en la UNE 19603 de Sistemas de gestión de compliance en materia de libre competencia? ¿Cuántas empresas auditan su gestión sociolaboral?

El mundo del Derecho es apasionante. Siempre habrá una pregunta más a la que buscar respuesta. A veces, lo difícil no es obtenerla sino tener la voluntad de aplicar una solución desde la perspectiva del Cumplimiento: no es fácil gestionar un sistema de Compliance cuando no existe el “tone from the top”.

Y mientras tanto, ¿Qué tal si se deja de mirar hacia arriba de una vez por todas y se comprenden las funciones de Cumplimiento? Los profesionales de Compliance estamos aquí con vocación multiplicadora, no nos vamos a extinguir, ya que precisamente, nuestra misión es contribuir a la sostenibilidad de los negocios, eso sí, teniendo en cuenta que, ¡No todo vale!



EN LA SOMBRA DE LAS CRIPTOMONEDAS Y DEL METAVERSO

LA IMPERANTE NECESIDAD DE PROCEDIMIENTOS INTERNACIONALES CONTRA EL BLANQUEO DE CAPITAL EN ESTOS ECOSISTEMAS.



Luis Rodríguez Soler

CEO en Complianzen y Head Compliance en CE Consulting

En el universo digital de las criptomonedas y los criptoactivos, donde la libertad financiera se entrelaza con la opacidad, o presunta opacidad de cada transacción, una amenaza persistente se esconde en las sombras: el blanqueo de capitales. La necesidad urgente de establecer procedimientos internacionales para prevenir este delito financiero se manifiesta a través de casos emblemáticos y un llamamiento unísono de la comunidad global.

La pregunta del millón que cualquier curioso de este ecosistema se hace es siempre ¿Cuánto influye en la volatilidad de los precios de los criptoactivos las inyecciones de dinero de toda procedencia y cuanto influye la ley de la oferta y la demanda y la minería internacional de estos activos digitales?

Ya es tarde, obviamente, para limpiar la ingente cantidad de dinero de origen ilícito que propicia las constantes oscilaciones que se producen día a día en las revaluaciones y devaluaciones de los millares de cripto activos que pueblan este indefinido ecosistema; pero no lo es para frenar su contaminación en un universo post pandémico donde el uso de dinero fiat físico en soporte papel (billetes y monedas) es ya más propio de siglos pasados, conviviendo con el dinero más profusamente utilizado, el dinero

de toda índole y valores digitalizados.

Por ello nunca es tarde para comenzar de forma contundente a querer comprender de con una visión global que este universo vivirá en el futuro con mayor consolidación que lo hace desde hace más de 10 años en el mundo.

Si bien a la fecha no hay evidencia sólida que respalde de forma contundente la manida afirmación de que un alto porcentaje del valor de los criptoactivos y criptomonedas se debe principalmente al dinero fiat de origen ilícito, las oscilaciones en los valores de estas monedas digitales pueden atribuirse a una variedad de factores, y es importante no generalizar ni asumir motivos sin fundamentos.

A continuación, presento algunas reflexiones deductivas de las oscilaciones en los valores de criptoactivos, sin centrarse específicamente en el origen ilícito del dinero fiat, a saber.

Si nos fijamos en la adopción y demanda fluctuante de los diversos criptoactivos, los mismos son relativamente nuevos en comparación con las monedas tradicionales. Su adopción y aceptación en la sociedad influyen directamente en su demanda y, por ende, en su valor. Generaciones más jóvenes se mezclan con las más tradicionales, y las más informadas

con las menos, pero un alto porcentaje de la humanidad, sobre todo en épocas de tipos de interés bajos en el mundo fiat, buscan mayores rentabilidades, allá donde sea, sin meditar ni conocer a fondo las razones más lógicas de dichas rentabilidades.

Si miramos la materia desde el prisma de las regulaciones gubernamentales, podemos afirmar que las decisiones gubernamentales en torno a la regulación de criptoactivos pueden afectar significativamente su valor. Tanto los anuncios de prohibiciones como de apoyos a unos y otros criptoactivos pueden generar fuertes fluctuaciones en sentidos opuestos. Escándalos de actuaciones ambiciosas descontroladas enmascaradas en este nuevo ecosistema propician que subidas y bajadas de valor descomunales afloren en los medios en este universo no completa ni ciertamente regulado.

Esas noticias y eventos del mercado cripto y anuncios relacionados con la seguridad, asociaciones empresariales, mejoras tecnológicas y otros eventos pueden influir en la percepción del mercado sobre la viabilidad y utilidad de cualquier criptomoneda o criptoactivo.

La volatilidad inherente a estos instrumentos digitales y la falta de respaldo



físico, la ausencia de regulaciones establecidas y la relativa novedad de las mismas pueden contribuir a la volatilidad inherente de sus valores.

Otro factor fundamental que también ocurre en los mercados de valores regulados es las manipulaciones del mercado. Si bien la especulación y la manipulación del mercado por parte de inversores grandes pueden tener un impacto sustancial en los precios en títulos de mercados regulados, en el ecosistema cripto, donde en la actualidad es todo más parecido a una selva sin reglas, estas manipulaciones obran con efecto multiplicador. Operaciones masivas de compra o venta de criptos provocan cambios bruscos en sus valoraciones.

La tecnología subyacente del ecosistema cripto es quizá el factor fundamental que provoca esta revolución. Cambios vertiginosos en la tecnología subyacente de una criptomoneda, como actualizaciones de protocolos o problemas de seguridad, pueden influir en la percepción del mercado y afectar a su valor. Si bien puede haber casos aislados de uso de criptomonedas en actividades ilícitas, no hay evidencia convincente que respalde la afirmación de que la mayoría del valor de las criptomonedas proviene de dinero FIAT de origen ilícito. Es crucial basarse en información respaldada por pruebas y evitar generalizaciones infundadas al analizar las causas de las oscilaciones en el mercado de criptomonedas.

Por todo lo que antecede, opino que afrontar la legislación en materia de prevención de blanqueo de capitales -quizá

el riesgo delictivo más evidente en esta industria- en el universo de criptoactivos con un enfoque exclusivamente nacional, regional o local es un enfoque erróneo y miope por varias razones fundamentales que expongo a continuación.

La naturaleza global de las criptomonedas y criptoactivos que operan en un entorno descentralizado y global hacen que sus transacciones no reconozcan fronteras nacionales, lo que hace que cualquier intento de regulación a nivel exclusivamente local, nacional, o regional sea incompleta e ineficaz. Un marco regulatorio localizado no puede abordar eficazmente las transacciones que trascienden las jurisdicciones.

Un enfoque puramente local o nacional crea el que podemos denominar "Riesgo de Desplazamiento", un riesgo de que las actividades ilícitas se desplacen hacia áreas con regulaciones más laxas o inexistentes. Los actores malintencionados pueden fácilmente trasladar sus operaciones a jurisdicciones con menos restricciones, eludiendo así las medidas preventivas implementadas a nivel local.

Asimismo, la variedad y desconexión entre normativas locales propicia que las regulaciones sobre criptoactivos varíen significativamente entre diferentes países y regiones. La falta de armonización crea lagunas y ambigüedades, dificultando la aplicación coherente de medidas de prevención del blanqueo de capitales y financiación de posibles actividades terroristas o de células que las apoyan.

Propongo por ello algunas reflexiones que nos llevarían al desarrollo de un

marco preventivo más adecuado en dicho contexto.

La necesidad de una colaboración real y práctica de ámbito internacional es clave en este nuevo ecosistema. El blanqueo de capitales es un problema global que requiere una respuesta global. La coordinación entre países es esencial para compartir información, identificar patrones transnacionales y tomar medidas conjuntas. Sin esta colaboración, se debilita la capacidad de hacer frente a las complejidades de las operaciones ilícitas. La colaboración silente y oscura de grandes poderes fácticos en altas esferas transnacionales de muchos grandes bancos internacionales siguen operando de forma deliberadamente opaca. No expreso tal reflexión como si fuera un "conspiranoico". Hablo con fundamento y sin apelar a posibles mitos más propios de novelas de ciencia ficción o espionaje clásico.

El ecosistema cripto y las tecnologías blockchain llevan operando en la humanidad más de un decenio y sin embargo es en estos años post pandémicos cuando parecen haber aflorado al conocimiento básico universal como si fuesen una novedad.

Convive, de forma alarmante, el desconocimiento masivo, con otras olas de seguidores que parecen conocer y dominar estos ecosistemas a la par que hordas de personas que hablan de ello sin siquiera conocimientos básicos por considerarlo una materia de "moda". Y en este río revuelto es donde el crimen organizado y sobre todo, sus tentáculos más informados, encuentran un caldo de cultivo perfecto para ocultar, enmascarar, invertir y mezclar sus abundantes fondos de origen ilícito y en el peor de los casos, criminal.

En la fecha en que escribo este artículo el número de criptomonedas actual se estima en más de 9.000, siendo el Bitcoin una de ellas, la más famosa. Esto puede darnos una idea del desconocimiento e incertidumbres a que la humanidad todavía nos enfrentamos en este campo. En España, por ejemplo, a esta misma fecha, sólo el 16% de la población afirma poseer criptomonedas. A nivel mundial, de los 8 mil millones de personas que poblamos el planeta, solo 100 millones de personas dicen poseer Bitcoin a 2023, es decir sólo el 1,25% de la población mundial. Pero ¿podemos considerar como cierta esta afirmación? Obviamente no lo creo. Muchos miles, no lo confiesan por vergüenza o discreción, otros muchos por incertidumbre en la re-

acción de quien pregunte y los más oscuros y poderosos no lo hacen porque el mayor volumen de dinero FIAT incorporado a estos ecosistemas lo han hecho para ocultar o almacenar con fines muchas veces meramente especulativos sus fondos de origen ilícitos, máxime en un mundo donde cada día es más habitual percibir que el dinero físico en monedas y billetes, y sobre todo los de alta denominación facial, billetes de 500 o 200 Euros, tiene sus días contados... por su cada vez más limitado uso en tráfico legal.

Para hacernos una idea aproximada, las fuentes más fiables muestran que la capitalización de mercado total del mercado de criptomonedas superó los USD 1.55 billones el 5 de diciembre 2022, siendo 2023 un año donde sigue progresando la consolidación del ecosistema a pesar de ciertos sonados escándalos que apuntaremos en este artículo.

Todos estos datos nos hacen pensar que, si bien los volúmenes financieros asociados a este ecosistema son descomunales e inciertos, por no ser obviamente certificables ni auditables por entes externos, si bien sí lo son en sus propias cadenas de configuración, y sabiendo que llevamos ya conviviendo más de 10 años con ellos, estamos realmente, como percibe la mayoría de la población mundial, en los inicios de su proliferación.

Otro factor clave en este ecosistema, sería la rapidez en la evolución tecnológica que estamos viviendo en el siglo XXI. La tecnología subyacente de las criptomonedas está en constante evolución. Un enfoque exclusivamente local puede quedar obsoleto rápidamente a medida que surgen nuevas formas de transacciones y se desarrollan tecnologías financieras emergentes. Un marco internacional de consenso, aunque fuese incipiente, y "en lo básico" puede adaptarse mejor a estos cambios dinámicos que soluciones miopes locales o regionales, pero precisa de un estudio riguroso y pormenorizado de los políticos y sus equipos de tecnócratas encargados de tales tareas.

El fortalecimiento de la confianza del usuario es otra de las asignaturas pendientes que debemos considerar. Los usuarios de criptomonedas valoran la seguridad y la transparencia, la independencia, la privacidad y la libertad. Un enfoque global fortalece la confianza al ofrecer un marco regulatorio coherente y predecible. La falta de uniformidad puede generar incertidumbre entre los

participantes del mercado, afectando negativamente la adopción y el crecimiento sostenible del ecosistema criptográfico.

Es sin embargo la inclusión de actores externos la materia que estimo posiblemente más complicada de gestionar. Dado que las criptomonedas y cryptoactivos no están limitados a actores tradicionales del sistema financiero, como bancos y otras instituciones financieras, es fundamental involucrar a plataformas de intercambio, billeteras digitales y otros servicios Fintech relacionados en un marco regulatorio global. Ignorar estos actores externos que son realmente quienes mejor conocen estos novedosos ecosistemas, limita la eficacia de cualquier medida adoptada a nivel local, y más basadas en promesas políticas poco fundamentadas muchas veces y desarrolladas en base a planteamientos teóricos.

En resumen, abordar la prevención del blanqueo de capitales en el universo de cryptoactivos requiere un enfoque internacional global (no local) y cohesionado, para garantizar la coherencia, la eficacia y la capacidad de adaptación a la naturaleza dinámica de este espacio financiero emergente. La cooperación global es esencial para abordar de manera efectiva los desafíos y riesgos asociados con las transacciones criptográficas. Pero no reglar desde un prisma unilateral y teórico. Al igual que en siglos pasados el paso del palo a la piedra, de la piedra al metal, del metal al oro y del oro al papel y del papel al bit, ahora toca profundizar en "los unos y los ceros" de una manera más sesuda para comprender que mientras conviva el FIAT en papel con un contexto universal digitalizado, le blanqueo será una lacra inevitable.

Miles de redes ocultas de transacciones

operan hoy en un ecosistema que clama por ser conocido y razonablemente regulado. Toda criptomoneda, con su promesa de transacciones rápidas y descentralización, ha brindado un terreno fértil para el blanqueo de capitales en la actualidad en este contexto, donde defraudadores fiscales a gran escala, promotores universales de economías sumergidas al margen del fisco, y todas las redes de tráfico ilegales, almacenan pallets de billetes de alta denominación que, si no les dan salida de forma urgente, pueden estar pudriéndose en oscuros almacenes. Cada día en cualquier parte del mundo, si bien no salen en los más relevantes titulares, se revelan redes clandestinas que utilizan criptomonedas para lavar miles de millones de dólares, euros o monedas Fiat actuales. La ausencia de regulaciones internacionales efectivas permite que estas redes operen impunemente, poniendo de manifiesto la necesidad de un enfoque unificado para enfrentar estos desafíos.

Algunas plataformas negligentes, operando en los mismos mercados que plataformas de intercambio de criptomonedas que desean hacerlo de forma legítima, conocidas por su papel crucial en la facilitación de transacciones, también han caído bajo el escrutinio. Varias de ellas, algunas de renombrada fama, como veremos más adelante, están siendo sancionadas por no implementar adecuadamente medidas contra el blanqueo de capitales. Esto resalta la importancia de procedimientos internacionales que regulen estas plataformas y refuercen la seguridad del ecosistema criptográfico.

La falta de colaboración entre jurisdicciones nacionales ha permitido que el blanqueo de capitales se propague sin obstáculos. La propia Binance, como

veremos más adelante se ha enfrentado a críticas internacionales por su falta de acción y cooperación en la prevención de actividades ilícitas relacionadas con criptomonedas. Este caso subraya la necesidad de establecer puentes entre países y forjar una respuesta colectiva.

Frente a estos desafíos, la comunidad internacional reconoce cada vez más la necesidad de procedimientos internacionales que regulen el uso de criptomonedas. Organismos como el Grupo de Acción Financiera Internacional (GAFI) y la Financial Action Task Force (FATF) han estado trabajando en estándares y recomendaciones para abordar las lagunas existentes.

La implantación de procedimientos KYC (Conoce a tu Cliente) a nivel global, la supervisión constante de transacciones, con los recientes procedimientos de algunas consultoras especializadas como Complianzen con Wensys están promoviendo KYW (Know Your Wallet) para operaciones singulares o Chainalysis para transacciones masivas; y la colaboración estrecha entre reguladores son pasos esenciales en esta lucha.

Un enfoque tradicional en la prevención del blanqueo - donde se preste más atención al "quién" (KYC) que al "qué" (KYW) es totalmente errático en este ecosistema. El dinero, venga de donde venga y desde su creación hace siglos, realmente, en su propia esencia, es realmente anónimo. Ha sido la evolución de los Estados, los Gobiernos y de la Banca la que le puso nombres y apellidos al dinero...pero lo cierto es que, en esencia el dinero no tiene propietario unívoco. Esta "adopción" de correlacionar persona con dinero es un invento de la humanidad, presuntamente civilizada, con fines meramente recaudatorios y de índole fiscal.

La falta de un enfoque internacional sólido por tanto en este ecosistema, no sólo pone en peligro la integridad del sistema financiero, sino que también socava la confianza en las criptomonedas como una alternativa legítima de futuro.

Sirva el reciente y sonado Caso de BINANCE, como ejemplo de cómo un exchanger puede cumplir perfectamente con las reglas en una jurisdicción y ser sancionado por graves incumplimientos en otro país. En los últimos meses este acontecimiento ha puesto de manifiesto de manera contundente la necesidad de rigor en esta materia en este nuevo universo.

Changpeng Zhao, el fundador y Ceo del gigante de las criptomonedas Binance, decía a sus empleados que era "mejor pedir perdón que pedir permiso", según los fiscales. La plataforma puso el crecimiento y los beneficios por encima del cumplimiento de la ley. Ahora, ha aceptado pagar un alto precio por las irregularidades cometidas en Estados Unidos. La firma ha alcanzado un acuerdo con el Departamento de Justicia, el Tesoro y la Comisión del Mercado de Futuros (CFTC) para pagar una multa récord de 4.368 millones de USD (unos 4.000 millones de €) por violar las leyes contra el blanqueo de capitales y la regulación de los mercados de valores. Además, Zhao se ha declarado culpable de un delito y ha aceptado dimitir, pero podrá mantener el control accionario de la compañía.

Changpeng Zhao tuvo que comparecer en un juzgado federal de Seattle (Washington) para declararse culpable de un delito por no mantener un programa eficaz contra el blanqueo de dinero. Binance, el mayor mercado de criptomonedas del mundo a la fecha, actúa en Estados Unidos dependiendo de una sociedad de responsabilidad limitada de las Islas Caimán. El acuerdo incluye una multa personal a pagar por Zhao, pero sobre todo ese acuerdo de 4.368 millones de USD, que podría incrementarse en 150 millones más si Binance no cumple una serie de condiciones.

Binance es a la fecha la mayor bolsa de criptomonedas del mundo, responsable de aproximadamente el 60% de la negociación centralizada de criptodivisas al contado. El acuerdo se produce para compensar por violaciones de la Ley de Secreto Bancario (BSA) y aparentes violaciones de múltiples programas de sanciones. La plataforma falló al prevenir e informar de transacciones sospechosas con terroristas, incluidas las Brigadas Al-Qassam de Hamás, la Yihad Islámi-

ca Palestina (YIP), Al Qaeda y el Estado Islámico de Irak y Siria (ISIS). También operó con atacantes de ransomware, blanqueadores de dinero y otros delincuentes, y tampoco impidió operaciones entre usuarios estadounidenses y otros en jurisdicciones sancionadas como Irán, Corea del Norte, Siria y la región ucraniana de Crimea, según el Tesoro americano.

"Binance hizo la vista gorda a sus obligaciones legales en su afán de lucro. Sus fallos deliberados permitieron que el dinero fluyera a terroristas, ciberdelincuentes y pederastas a través de su plataforma", ha declarado la secretaria del Tesoro, Janet Yellen, en un comunicado. "Las sanciones históricas de hoy y la supervisión para garantizar el cumplimiento de la legislación y la normativa estadounidenses marcan un hito para el sector de las criptomonedas", añadió.

El acuerdo de conciliación con la red del Tesoro contra los delitos financieros (FinCEN) supone una multa civil de 3.400 millones de USD, una supervisión de cinco años e importantes compromisos, incluido el de garantizar la salida completa de Binance de Estados Unidos. Es la mayor sanción en la historia del Tesoro de Estados Unidos y de la FinCEN. Además, el acuerdo con la Oficina de Control de Bienes Extranjeros (OFAC) suma otra multa de 968 millones de USD. Para garantizar que Binance cumple las condiciones de su acuerdo, incluida la de no ofrecer servicios a estadounidenses, y asegurarse de que se aborda la actividad ilícita, el Tesoro mantendrá el acceso a los libros, registros y sistemas de Binance durante un periodo de cinco años.

Una vez admitida su culpa por parte de Zhao, el juez ha fijado provisionalmente el 23 de febrero de 2024 como fecha para la sentencia de Zhao, aunque es probable que se retrase, ya que ambas partes acordaron que no habría condena durante al menos seis meses.

El sector de las criptomonedas ha visto ensuciada así su imagen por una sucesión de escándalos entre los que el más sonado fue la caída de FTX, plataforma rival de Binance, aunque ambas tuvieron negocios cruzados entre sí. El fundador de FTX, Sam Bankman Fried, fue declarado culpable el pasado 2 de noviembre de 2023 de siete cargos de fraude y conspiración por los que puede ser condenado a una pena máxima de más de 100 años de cárcel. El jurado rechazó la línea de defensa argumental del californiano, de 31 años, según la cual



no estafó a nadie y por eso rechazaba su culpabilidad, admitiendo solo errores de gestión.

Con todo lo que antecede, y sin menospreciar ni mucho menos estos sonados escándalos, lo que no debemos hacer es culpar al ecosistema. Un cuchillo sirve lo mismo para cortar alimentos de todo tipo... como sirve también para matar. Muchos agoreros, y presuntos "gurús de papel" o perezosos amantes torpes del sensacionalismo fácil de contextos "de moda" como es el que nos ocupa, critican el ecosistema cripto sin un mínimo rigor básico. Estos personajes, flor de un día, han visto en este nuevo escándalo un argumento más para frenar el avance de este ecosistema que nació hace más de una década y que no tiene visos de parar de crecer.

RETOS FUTUROS QUE HOY LOS COMPLIANCE OFFICER NI SE PLANTEAN...

Por último, como apasionado de este nuevo mundo que ha irrumpido en nuestra era, me aventuro a argumentar razones por las que preocuparse por los riesgos de blanqueo de capitales mediante uso de criptoactivos por el crimen organizado en el metaverso. Estos retos, a día de hoy, ni se encuentran en la hoja de ruta de los *preventores* tradicionales.

Expongo seguidamente las principales preocupaciones que podrían asociarse vinculadas a los riesgos de blanqueo de capitales mediante uso de criptoactivos por el crimen organizado en el metaverso. La razón es esencial debido a diversas razones que resaltan la necesidad de una atención especial y una regulación adecuada en este ámbito emergente.

Para aquellos que no estáis familiarizados con el término o lo estimáis como algo lejano y difuso por indefinido, comentaros que el metaverso es ya una realidad. El metaverso es un concepto que se refiere a un espacio virtual en línea donde las personas pueden interactuar entre sí y con contenido digital de una manera similar o incluso más compleja que en el mundo real. En el metaverso, puedes explorar entornos digitales, socializar con otras personas, participar en actividades recreativas, trabajar, realizar transacciones comerciales e incluso crear y modificar tu propia realidad virtual.

Imagina un universo digital expansivo que integra elementos de juegos, redes sociales, comercio, educación y más, todo en un solo lugar. Puedes tener tu

propio avatar, que es una representación digital de ti mismo, y moverte por este mundo virtual de una manera que va más allá de las experiencias en línea convencionales.

El término "metaverso" a menudo se asocia con la idea de una realidad alternativa en la que las personas pueden sumergirse, interactuar y participar activamente en diversas actividades. Este concepto ha ganado popularidad con el avance de la tecnología, la realidad virtual y la realidad aumentada, creando un espacio digital más inmersivo y diverso que lo que conocemos en internet hoy en día.

En el metaverso, las transacciones pueden ser realizadas de manera relativamente anónima, propiciando la opacidad y *pseudoanonimato*. Todo ello facilita a los actores del crimen organizado ocultar su identidad y blanquear fondos de manera más eficiente. La falta de regulaciones claras en este espacio puede dar lugar a una mayor explotación de esta característica para actividades ilícitas.

Las transacciones transfronterizas se realizan sin restricciones. El metaverso no está limitado por fronteras geográficas, permitiendo a los criminales mover fondos de manera rápida y sin restricciones entre diferentes plataformas y jurisdicciones. Esto crea desafíos significativos para la aplicación de leyes y regulaciones a nivel internacional. Además, la complejidad de las transacciones descentralizadas en el metaverso puede ser más difíciles de rastrear y regular debido a la ausencia de intermediarios centralizados. Esto proporciona a los actores del crimen organizado una mayor flexibilidad para realizar operaciones sin ser detectados.

Paso a detallar algunas de las actividades que el crimen organizado a la fecha actual perpetra en este nuevo ecosistema sin ningún tipo de limitaciones.

- El uso de activos virtuales es la "capa del disfraz": El crimen organizado puede utilizar activos virtuales, como criptoactivos y tokens no fungibles (NFT), para disfrazar el origen y destino de los fondos. Este tipo de activos pueden ofrecer una capa adicional de complejidad al seguir la pista de transacciones ilegítimas.
- Economías Paralelas en el Metaverso: Con el crecimiento de las economías virtuales en el meta-

verso, existe el riesgo de que el crimen organizado establezca operaciones y empresas ficticias para legitimar sus actividades ilícitas. Este fenómeno puede dificultar aún más la identificación de transacciones sospechosas.

- Integración de Finanzas Descentralizadas (DeFi): Las finanzas descentralizadas, una parte integral del metaverso, presentan riesgos adicionales. Los protocolos DeFi pueden utilizarse para realizar actividades de préstamo y transacciones sin la intervención de instituciones financieras tradicionales, lo que complica la supervisión y aplicación de las regulaciones contra el blanqueo de capitales.
- Nuevas Formas de Fraude y Estafas: En el metaverso, pueden surgir nuevas formas de fraude y estafas que involucren criptoactivos. El crimen organizado puede aprovechar estas oportunidades para realizar actividades fraudulentas, desde esquemas de inversión hasta ventas de bienes virtuales falsos.
- Falta de Concienciación y Preparación: Dada la novedad del metaverso y su rápido desarrollo, la falta de conciencia y preparación entre los reguladores y las fuerzas del orden puede resultar en un rezago significativo. Los esfuerzos para abordar el blanqueo de capitales en este entorno necesitan ponerse al día con la realidad en evolución del metaverso.

En resumen, si bien en la primera parte del artículo os alertaba de la falta de regulación necesaria en el ecosistema blockchain, imaginad la situación en este todavía más desconocido sistema como es el Metaverso. El reto de los legisladores es ingente...y percibo que por su parte desconocido en toda su dimensión.

Los riesgos de blanqueo de capitales en el metaverso por parte del crimen organizado destacarán, en una segunda fase, por la necesidad de una supervisión y regulación proactivas para abordar los desafíos únicos que presenta este nuevo y complejo entorno financiero virtual. La colaboración internacional y el desarrollo de marcos regulatorios adaptados son esenciales para prevenir y mitigar estos riesgos de manera efectiva.

Soy de los que piensan que criticar lo desconocido y hablar de algo desde el más puro desconocimiento no aporta nada y crea un ruido y contaminación innecesarios en un universo en plena expansión, que no ayuda al progreso en ningún sentido.

Si bien es cierto que el universo blockchain y todas sus derivadas ha irrumpido con contundencia en la Humanidad, como en su día lo hizo la imprenta, la máquina de vapor, la electricidad, el telégrafo y teléfono, por poner los avances más disruptivos de la Historia de la Humanidad reciente, también lo es que gran parte de esta humanidad, sin necesariamente asociarlo a edades del hombre concretas, ha dividido tradicionalmente al ser humano en tres claras categorías: los que saben de este ecosistema y/o muestran interés en aprenderlo, los que directamente no saben ni quieren saber y los que coquetean con él "tocando de oído". Estos últimos son los más perjudiciales para el desarrollo del mismo pues su ignorancia y pereza no es silenciosa, y provoca gran pérdida de tiempo en el resto de la población.

CONCLUSIÓN: ESTEMOS EN LA VANGUARDIA DE LA PREVENCIÓN... RACIONAL.

Siendo muy contundente en mis últimas reflexiones, me atrevo a aventurar que el blanqueo, dentro de unos años (o siglos) desaparecerá como delito porque el papel moneda habrá pasado a mejor vida.

Recordemos que el blanqueo es uno de los delitos más jóvenes de las legislaciones internacionales, creado por el hombre, con motivo del paso de la proliferación del dinero en soporte papel al dinero materializado de en forma elec-

trónica o digital... incluso años antes del nacimiento de internet. Es por ello que las reflexiones de este artículo no deben tomarse como un acto de frivolidad ni algo exótico.

Algunos se reirán, igual que lo hicieron hace años cuando me aventuré a profetizar que los billetes de 500 euros no tenían sentido y dejarían de emitirse... y así ocurrió . En España el Banco de España cesó la emisión de billetes de 500 euros en enero de 2019. Si bien éstos siguen siendo de curso legal, son en la actualidad de escasa circulación y pueden usarse como medio de pago... con habituales restricciones en establecimientos cada vez más escasos, o bien y como depósito de valor, es decir, para comprar y ahorrar, pero... ¿hasta cuándo?. Los existentes por tanto son de escaso curso legal y si se acumulan en pocas manos, en altas cantidades, no estimo que sean manos "demasiado limpias" en la actualidad.

El mundo está en un nuevo punto de inflexión sin precedentes. Las criptomonedas, con su potencial transformador, deben ser resguardadas contra la sombra del blanqueo de capitales, como delito a prevenir a la fecha, más probable. La adopción de procedimientos internacionales no sólo es una necesidad, sino una responsabilidad compartida por todas las naciones que aspiran a un futuro financiero "digital" seguro y transparente. La llamada es clara, los procedimientos

internacionales son la luz que disipa la oscuridad financiera. Es hora de que la comunidad global se una en la creación de un marco regulatorio universal o al menos armonizado, que proteja la esencia misma de las criptomonedas y los criptoactivos, asegurando que la promesa de un sistema financiero más equitativo no se vea empañada por las acciones de unos pocos sin escrúpulos.

Todo ello, es imperativo y la velocidad con que debe afrontarse, debería reforzarse sobremedida, pues la convivencia con el nuevo ecosistema, todavía más salvaje, más complejo, como es el metaverso, debería "pillar" a la humanidad preparada. Si no, el caos se adueñará cada vez más de las multimillonarias relaciones que día a día acontecen y nos interconectan a toda la Humanidad en nuestro planeta.

Es, considero, el sector privado y empresarial y financiero el que deberá también seguir dichas reglas y leyes cuando estas se promulguen, y ser rigurosos y ejemplares en ello.

Y ante este reto descomunal, otra sombra acecha. El posible error de dejar todo en manos de estos nuevos ecosistemas y la cada vez más asentada inteligencia artificial, ante la más que posible ocurrencia de BlackOuts masivos o incluso uno global , universal... pero esta, sería otra historia que plantearé en un posible artículo en 2024.



OPTIMIZACIÓN DEL TAX COMPLIANCE A TRAVÉS DE LA IA



Franklin Martín Ruiz Gordillo

Agente del Ministerio Público - Fiscalía General del Estado de Oaxaca
Ex director de Gestión Administrativa y Educativa de la Coordinación General de Recursos Humanos de la Secretaría de Hacienda del Estado de Chiapas.

El 2022 terminó con uno de los lanzamientos más importantes en el contexto de la inteligencia artificial, el denominado ChatGPT, un sistema de redes neuronales con capacidades de aprendizaje profundo que representa uno de los mayores alcances del machine Learning en materia de detección de irregularidades. El sistema puede resultar muy útil, en materia de prevención delictiva y adecuado control interno asegurando la debida diligencia a partir de sistemas inteligentes respaldados por cadenas de bloques (*blockchain*), de manera que se cubre el valor preventivo que tiene el *tax compliance*.

EL COMPONENTE COGNITIVO DE LA IA Y SU ALCANCE EN LA PREVENCIÓN DELICTIVA

Desde el punto de vista jurídico, la Inteligencia Artificial se mantiene bajo una programación de aprendizaje continuo, es decir, que las cualidades cognitivas de las programaciones que se basan en redes neuronales y aprendizaje profundo deben realizar acciones inteligentes de prevención delictiva, e incluso de detección de errores en la relación jurídico tributaria; ya que como lo señala el Consejo de Estabilidad Financiera: "La IA es el conjunto de teorías y algoritmos que permiten que las computadoras lleven a cabo tareas que, típicamente, requieren capacidades propias de inteligencia humana como por ejemplo la percepción visual, el reconocimiento de voz o la interpretación de un texto teniendo en cuenta el contexto en el que se produce, y en ocasiones mejoran dichas capacidades"

El enfoque de la IA es predictivo, es decir que se anticipa a eventos futuros, a través del reconocimiento de patrones de conducta.

Como señala Bedolla Cesto (2019), estos algoritmos avanzados pueden reducir significativamente la cantidad de alertas falsas al filtrar los casos que se marcaron incorrectamente, al mismo tiempo que descubren otros que no se detectaron con las reglas convenciona-



les.

El Machine Learning, es un mecanismo del IA que se encarga de la detección de patrones presentes en los datos, su objetivo reside además en el desarrollo de algoritmos con valor práctico como el tiempo de ejecución, el espacio utilizado y la cantidad de datos empleados; ya que entre más robusto sea la *big data* se podrán identificar patrones con mayor soporte.

HERRAMIENTAS DE IA QUE PUEDEN INCLUIRSE EN EL PROGRAMA DE CUMPLIMIENTO TRIBUTARIO

En materia de redes neuronales, aprendizaje profundo, inteligencia artificial y

sistemas de prevención con características cognitivas se ha dado un avance enorme a partir del 30 de noviembre de 2022, momento en el que se presenta una de las innovaciones tecnológicas cuyo comportamiento es difícil de predecir, la empresa OpenAi lanza la herramienta Chat Generative Pre-training Transformer (ChatGPT), que Wenth (2023) define como "un tipo de inteligencias artificial (IA) generadora de voz y texto que permite conversaciones de chat similares a las humanas. Se utiliza habitualmente en aplicaciones y servicios de *Chatbot* para ayudar a usuarios a responder preguntas y resolver problemas."

Este modelo de procesamiento de len-

guaje utiliza una combinación de técnicas de *Deep Learning*, consiguiendo habilidades lingüísticas y capacidades cognitivas. Sobre de estas capacidades Ramos (2023) señala que: La IA se entrena con grandes cantidades de texto y datos para poder responder preguntas y generar textos coherentes en una amplia variedad de tareas y contextos; como resultado es capaz de comprender el contexto de una pregunta o tarea y proporcionar respuestas o textos precisos y convincentes.

Se habla de un fenómeno mundial derivado de que sus alcances han superado las expectativas para su calidad, ya que este modelo de IA es tan solo un prototipo de una sola empresa (Bing) en un campo que es dominado por empresas como Google, misma que ya ha presentado al llamado "Bard", que a pesar de no ser lanzado de manera oficial, es también un sistema conversacional, basado en *Language Model for Dialogue Applications* (LaMDA) que es un modelo de lenguaje experimental, conectado constantemente a Internet (a diferencia de ChatGPT).

DINÁMICA Y FLEXIBILIDAD NECESARIA EN LA NORMATIVIDAD EN MATERIA DE INTELIGENCIA ARTIFICIAL

La IA ha demostrado su capacidad para revolucionar procesos, optimizar tareas y ofrecer soluciones innovadoras, sin embargo, este rápido progreso tecnológico plantea desafíos significativos en términos de regulación y marcos normativos; el corazón de esta revolución tecnológica radica en la capacidad de la IA para aprender y adaptarse. Cada avance tecnológico, cada nueva característica añadida a los sistemas de IA, plantea interrogantes éticos y legales que el marco normativo actual debe abordar. ¿Cómo regular la IA cuando su capacidad de aprendizaje es constante y su evolución impredecible?

El desafío es claro: el marco normativo existente, aunque fundamental, no puede mantenerse estático en un mundo de avances exponenciales ante la IA. La regulación debe tener la capacidad de evolucionar en paralelo a la tecnología misma. La dinámica y flexibilidad en las normativas se vuelven esenciales para adaptarse a los cambios que la IA experimenta constantemente.

Uno de los principales aspectos a considerar es la transparencia en los algoritmos de IA, a medida que estos sistemas se vuelven más complejos, es crucial

comprender cómo toman decisiones. La rendición de cuentas y la explicabilidad en los procesos de toma de decisiones se convierten en pilares fundamentales para garantizar la confianza y la ética en su aplicación.

Además, la privacidad y la seguridad de los datos son temas cruciales en la regulación de la IA. Las normativas deben proporcionar un equilibrio entre el uso efectivo de los datos y la protección de la privacidad individual. La implementación de medidas que salvaguarden la información se vuelve cada vez más urgente a medida que la IA se integra en una mayor cantidad de sectores.

No obstante, la agilidad en la regulación no implica una falta de control. Al contrario, requiere una comprensión profunda de las capacidades y limitaciones de la IA. La colaboración entre expertos en tecnología, ética, legislación y sociedad se convierte en un aspecto clave para desarrollar normativas que sean equitativas, eficientes y adaptativas; el desafío para los legisladores y reguladores es encontrar el equilibrio adecuado: una regulación que fomente la innovación y el progreso tecnológico, al tiempo que garantice la ética, la transparencia y la seguridad en el uso de la IA. **Es crucial alcanzar un equilibrio: no excederse para no sofocar la innovación, pero tampoco quedarse rezagado de tal manera que las leyes carezcan de efectividad.**

LA ÉTICA EN LA PROGRAMACIÓN DE LA IA

El uso del aprendizaje profundo (*deep learning*), en la IA posibilita el procesamiento automatizado de grandes volúmenes de datos, lo que facilita la identificación de riesgos potenciales y respalda la toma de decisiones basadas en información objetiva, esto representa un avance muy notable en la eficiencia y efectividad de los mecanismos de supervisión y control empresarial.

La IA se muestra particularmente beneficiosa en la detección de posibles violaciones de normativas y regulaciones en vigor, por ejemplo identificando, a través de análisis de datos, comportamientos que sugieran la posible comisión de delitos, contribuyendo a la elaboración de informes de evaluaciones de riesgos, y facilitando así la toma de decisiones en los procesos de control y supervisión.

La implementación de la IA en el ámbito del cumplimiento normativo enfrenta desafíos y limitaciones considerables, uno de los principales desafíos radica en el

riesgo de que los resultados generados por esta tecnología presenten sesgos o discriminación, por tanto, resulta fundamental asegurar la ética en los algoritmos utilizados, evitando cualquier tipo de perjuicio hacia individuos, grupos e incluso sectores en última instancia. Este aspecto ético se convierte en un punto crucial para mantener la integridad y la equidad en la aplicación de la IA en entornos regulatorios y empresariales.

EL COOPERATIVE TAX COMPLIANCE PUBLICADO POR LA OCDE Y LA IA.

El Informe "Co-operative Tax Compliance" publicado por la OCDE en 2016 es un punto de referencia fundamental en la discusión sobre la transparencia y el cumplimiento tributario. Este informe, fruto del trabajo de expertos fiscales de diversos países como Australia, Canadá, Finlandia, Francia y México, planteó la idea de que una mayor transparencia en la relación con las autoridades tributarias podría disminuir la necesidad de verificaciones exhaustivas de las declaraciones fiscales. Se sugiere que esta transparencia mejoraría la fiabilidad de las declaraciones y, como resultado, reduciría los costos y aumentaría el cumplimiento.

El informe propone acciones específicas para lograr este cumplimiento tributario cooperativo, entre las que se encuentran cambiar la seguridad jurídica por transparencia, desarrollar métodos internos de evaluación de riesgos y crear guías adicionales para identificar riesgos fiscales.

Se destacan principios clave que sustentan este enfoque, como establecer estrategias fiscales definidas por órganos ejecutivos y asignar responsabilidades al Consejo de Administración para implementar medidas de seguridad fiscales. Asimismo, enfatiza la importancia de una gobernanza fiscal documentada y verifica continua tanto interna como externamente para fortalecer el sistema y gestionar riesgos de manera efectiva.

Se hace énfasis en el fortalecimiento de los mecanismos de buen gobierno corporativo mediante el uso de tecnología para identificar y analizar en tiempo real las inconsistencias fiscales. Y precisamente las características de la IA favorecen su uso como herramienta para lograr los objetivos del tax Compliance, tales como:

- **El análisis avanzado de datos:** Las herramientas de IA pueden

procesar grandes volúmenes de datos fiscales para identificar posibles incongruencias o anomalías en las declaraciones, ayudando a detectar patrones irregulares que podrían indicar evasión fiscal o errores involuntarios.

- **La automatización de procesos:** Se automatizan ciertos procesos relacionados con la evaluación de riesgos fiscales y la identificación de áreas que necesitan atención, lo que agiliza el proceso y reduce errores humanos.
- **La mejora de la predicción:** La IA puede mejorar la precisión en la predicción de riesgos fiscales al identificar correlaciones y patrones que pueden no ser evidentes para los analistas humanos, lo que permite una toma de decisiones más fundamentada.
- **La adaptación a los cambios normativos:** Los sistemas de IA pueden ser flexibles y adaptarse a cambios en las leyes fiscales, actualizándose automáticamente para reflejar las nuevas regulaciones y asegurando que se sigan los procedimientos adecuados.

La relación entre el informe de la OCDE y la implementación de herramientas de IA en el ámbito tributario resalta la importancia de utilizar la tecnología para mejorar la transparencia, el cumplimiento y la eficiencia en la gestión fiscal (control interno); la combinación de prácticas de cumplimiento tributario cooperativo con soluciones de IA puede ser fundamental para lograr sistemas fiscales más transparentes, confiables y eficaces.

GOBERNANZA DE LA INTELIGENCIA ARTIFICIAL EN LA EMPRESA

Las brechas en la seguridad de los datos no solo pueden dañar la reputación corporativa, sino también generar consecuencias legales y pérdidas financieras significativas. Un riesgo crítico asociado a los datos es la presencia de sesgos en los algoritmos utilizados en sistemas de IA, estos algoritmos aprenden de los datos con los que se entrenan y, si estos datos contienen sesgos, pueden conducir a resultados no deseados o incluso perjudiciales.

Es esencial comprender que una implementación descuidada o inapropiada de la IA puede exponer a las organizaciones a riesgos operativos, financieros, regulatorios y de reputación, por lo tanto, es

tablecer sólidas salvaguardias se vuelve imperativo para asegurar el correcto funcionamiento de estas soluciones. Esto implica la creación de un robusto marco de gobernanza que se adapte a las particularidades y capacidades de la IA.

La gobernanza de la IA abarca la formulación de políticas y la asignación de responsabilidades para impulsar el desarrollo y uso adecuado de sistemas de IA en las organizaciones. Este marco integral se enfoca en la gestión de riesgos, el cumplimiento normativo, los acuerdos contractuales y aspectos éticos relacionados con el uso de esta tecnología.

Cuando se implementa de manera efectiva, la gobernanza de la IA no solo impulsa la agilidad organizativa, sino que también fomenta la confianza en estas soluciones. En la actualidad, existen múltiples alcances de la IA en materia de control interno y más precisamente del tax Compliance, entre estos se encuentran:

- **Detección de anomalías.** Uno de los aspectos más destacados de la IA en el control interno es su capacidad para detectar anomalías. A través del análisis de grandes volúmenes de datos en tiempo real, la IA puede identificar patrones irregulares o transacciones sospechosas. Esta habilidad permite a las organizaciones prever posibles fraudes o fallas en los procesos internos, lo que les brinda la oportunidad de intervenir de manera inmediata para evitar pérdidas significativas. Por ejemplo, en una institución financiera, si se detecta un patrón inusual en las transferencias de fondos, la IA alerta al equipo de control interno, lo que permite una rápida intervención y prevención de actividades fraudulentas.
- **La automatización de procesos de control** es otro beneficio clave de la IA en el ámbito del control interno que posibilita la ejecución eficiente y precisa de tareas rutinarias como la conciliación de datos y la verificación del cumplimiento normativo. Al liberar al personal de tareas repetitivas, la IA reduce la probabilidad de errores humanos y permite que los equipos se concentren en labores estratégicas. Por ejemplo, en la reconciliación de datos contables, la IA identifica discrepancias, realiza ajustes y genera informes precisos, lo que mejora la confiabili-

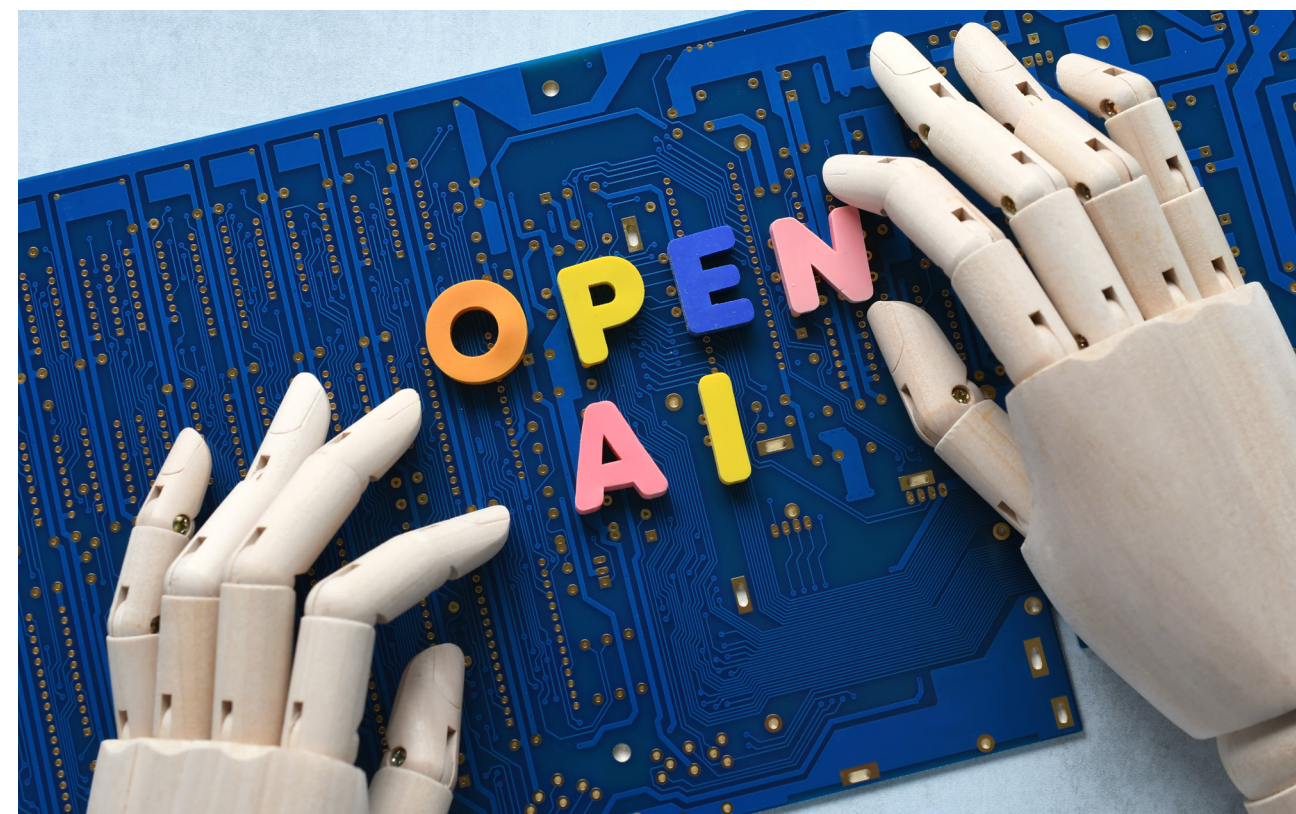
dad de la información financiera.

- **La capacidad predictiva de la IA es una herramienta valiosa para anticipar riesgos futuros.** Los algoritmos de aprendizaje automático tienen la habilidad de analizar patrones históricos y prever posibles situaciones de riesgo antes de que se conviertan en problemas significativos. Por ejemplo, en compañías de seguros, la IA puede detectar patrones que sugieren un aumento en ciertos tipos de reclamaciones, lo que permite a la empresa adaptar sus estrategias de gestión de riesgos y establecer medidas preventivas.
- **En cuanto a la seguridad cibernética,** la IA desempeña un papel crucial en la **detección de comportamientos maliciosos y la identificación de vulnerabilidades en tiempo real.** Esto asegura una protección efectiva de los sistemas internos contra posibles amenazas y violaciones de seguridad.

REDUCCIÓN DE CARGAS PENALES A PARTIR DE LA CAPACIDAD PREDICTIVA DE LA IA EN EL CONTROL INTERNO DEL TAX COMPLIANCE

La noción de autorresponsabilidad en el ámbito de las personas jurídicas ha cobrado una significativa relevancia en el contexto jurídico de México y de España, entre otros países de la OCDE. Este enfoque establece modelos donde la responsabilidad penal de la persona jurídica se asocia con fallas en su estructura organizativa y falta de apego a la legalidad o cultura de cumplimiento. Esta perspectiva se basa en la premisa fundamental de que una empresa, como entidad colectiva, no puede ser equiparada a un individuo en términos de culpabilidad penal.

El modelo de autorresponsabilidad, sustentado en el Artículo 421 del Código Nacional de Procedimientos Penales en México, y en la interpretación que, tras superar ciertas dudas, la Fiscalía General del Estado y el Tribunal Supremo Españoles han realizado del art. 31 bis del Código Penal Español, establece la responsabilidad penal autónoma de la persona jurídica en función de sus propias acciones, independientemente de las responsabilidades individuales de sus representantes o administradores. Esta concepción se dirige hacia la idea de un Delito Corporativo, donde las acciones



se ejecutan en beneficio de la entidad, a su nombre o mediante sus recursos, evaluándose a través de la insuficiencia en su estructura organizativa.

El ilícito específico atribuido a una persona jurídica abarcará cualquier defecto que se manifieste dentro de su estructura organizativa. Si bien es claro que la entidad legal no tiene la misma capacidad de acción que un individuo, su equivalente funcional en términos de la teoría del delito será su capacidad de organización.

Cuando se detecte un defecto en la empresa que cause o no evite daños previsible y evitables por falta del debido control a un bien jurídico penalmente protegido, se considerará la conducta antijurídica punible (el ilícito a nivel objetivo). En términos de la culpabilidad exigible para sancionar penalmente la conducta ilícita de la persona jurídica, se exigirá la falta de apego a la ley, o "falta de cultura de cumplimiento" en palabras utilizadas por el Tribunal Supremo español, materializada en un incumplimiento voluntario de los deberes y obligaciones impuestos por la ley. Por lo tanto, para establecer la responsabilidad de la entidad legal, se deben llevar a cabo ambos juicios, el primero es sobre el acto en sí, que se fundamenta en el fallo dentro de la estructura organizativa, y en segunda instancia, sobre la culpabilidad de la persona Jurídica, que implica la falta de apego a las normas legales en vigor.

Este enfoque de autorresponsabilidad representa la postura doctrinal asumida tanto por el Código Penal Español interpretado por el Tribunal Supremo como por el Código Nacional de Procedimientos Penales que conceptúan el Delito Corporativo como aquel cometido en nombre de la entidad legal, por su cuenta, en su beneficio o a través de los medios que proporciona, cuando también se ha determinado una falta de control adecuado en su estructura organizativa, y ello independientemente de la responsabilidad penal en la que puedan incurrir sus representantes o administradores legales o de hecho.

No obstante, este planteamiento enfrenta desafíos inherentes, como la imposibilidad de atribuir a la organización una culpabilidad similar a la de un individuo, debido a su carencia de autonomía para generar actos delictivos. Su papel se limita a crear condiciones que puedan propiciar, en un contexto criminógeno, la comisión de delitos individuales. Además, la estructura organizativa depende de la participación de sus miembros y no actúa de manera autónoma.

En consecuencia, el modelo de responsabilidad penal de la persona jurídica se refiere más a su déficit estructural que a la producción directa de resultados (lo que sí ocurre en casos de sociedades instrumentales para delinquir). Esta responsabilidad estructural se vincula con la capacidad de la organización para in-

fluir en los actos individuales y la medida en que haya contribuido a un entorno propenso a la comisión de delitos.

En síntesis, el modelo de autorresponsabilidad adoptado busca asignar responsabilidades a la entidad jurídica basándose en su estructura y su influencia en los actos individuales.

CONCLUSIONES

- La integración de la Inteligencia Artificial en el ámbito del cumplimiento tributario introduce una nueva era donde se minimizan los errores imprevistos o no calculados, este avance se apoya en un continuo proceso de aprendizaje, respaldado por las capacidades cognitivas de la programación, basadas en redes neuronales y aprendizaje profundo. La finalidad es ejecutar acciones inteligentes que van desde la prevención de conductas ilegales hasta la detección de errores en los ámbitos legales y tributarios.
- El enfoque primordial de la IA es predictivo, lo que implica su habilidad para anticipar eventos futuros mediante el reconocimiento de patrones de comportamiento. Las soluciones actuales de aprendizaje utilizan reglas predictivas que identifican automáticamente anomalías en conjuntos de datos,



reduciendo las alertas falsas y descubriendo casos que podrían pasar desapercibidos con reglas convencionales.

- La identificación automática de anomalías, impulsada por IA como las redes neuronales artificiales, se traduce en sistemas de respuestas basados en reglas binarias.
- El aprendizaje automático se dedica a detectar patrones presentes en los datos y desarrollar algoritmos prácticos, considerando aspectos como el tiempo de ejecución, el espacio utilizado y la cantidad de datos empleados. Su capacidad para identificar patrones se fortalece con una base de datos más robusta. En la actualidad, el análisis predictivo y proyectivo ha adquirido una importancia crucial en la gestión de mercados y la administración empresarial debido a los avances tecnológicos. La ciencia de datos y los algoritmos aplicados para la toma de decisiones, vinculados a fuentes gubernamentales y de mercado, han transformado el uso de las matemáticas en la predicción aplicada en la gestión empresarial y la gestión de riesgos, esto emergiendo del big data o ciencia de datos.
- El propósito fundamental de la aplicación de algoritmos en la gestión empresarial es automa-

tizar procedimientos para analizar parámetros relevantes en la toma diaria de decisiones de los directivos, proporcionando resultados y orientación sobre las acciones a tomar. La toma de decisiones empresariales, especialmente en la gestión de riesgos, se basa en el análisis de diversos factores, como el historial de deudas, la participación en el mercado y la diligencia debida.

- La IA, respaldada por la aplicación de algoritmos, contribuye a responder a las condiciones contextuales a través de mecanismos internos, acelerando los tiempos de ejecución e implementación. Sin embargo, las organizaciones que adoptan estos enfoques avanzados enfrentan desafíos, incluyendo la calidad y validación de datos, la gestión de información sensible y el cumplimiento de los requisitos regulatorios.

Esto quiere decir que su sistema puede basarse exclusivamente en responder a las normativas en materia tributaria e identificar anomalías a partir de la programación y aprendizaje cognitivo en donde una de sus fuentes sería el propio internet; por lo que ahora se deben manifestar acciones que brinden certeza y seguridad jurídica de que no serán violentados estos sistemas inteligentes, situación que también ha sido considerada a partir del *block-*

chain; por lo que la programación inteligente parece estar de lado de la prevención delictiva, misma que estará a disposición solo de aquellos que tengan la capacidad de adjudicarlos e implementarlos en sus sistemas operativos.

Cabe señalar que si una empresa implementa un sistema de IA en su control interno para prevenir fraudes o gestionar riesgos, la manera en que se diseña este sistema y se integra en la estructura organizativa podría influir en las decisiones tomadas por los individuos que interactúan con él. Si este sistema de IA no está adecuadamente configurado, podría propiciar un entorno propenso a ciertas prácticas o acciones que, aunque no sean ilícitas por sí mismas, podrían derivar en resultados no deseados o en actos indebidos.

- Asimismo, la responsabilidad estructural de una empresa frente a la IA puede recaer en la forma en que se establecen los controles, la supervisión y el diseño de la tecnología. Si la IA se utiliza de manera inadecuada o si no se implementan los mecanismos de control necesarios para mitigar riesgos asociados con su uso, la empresa podría ser considerada responsable en la medida en que proporciona un contexto que podría propiciar acciones irregulares por parte de los individuos que interactúan con esta tecnología.

REFERENCIAS

- Bedolla Cesto, E. (21 de Junio de 2019). Ciberseguridad. Recuperado el 10 de Mayo de 2022, de Riesgos y beneficios pde usar las IA para detectar delitos: https://ciberseguridad.com/guias/nuevas-tecnologias/inteligencia-artificial/detectar-delitos/#%C2%BFCual_es_el_papel_de_la_IA_en_el_Derecho_penal
- Consejo de Estabilidad Financiera. (2017). *Artificial intelligence and machine learning in financial services*. EEUU: CEF.
- Ramos, J. (2023). *ChatGPT para la Educación del Siglo XXI*. México: XinXii.
- Trujillo Fernández, D. (2017). *Aplicación de metodologías Machine Learning en la Gestión de Riesgo de Crédito*. Madrid, España: Universidad Politécnica de Madrid.
- Wenth, A. (2023). *ChatGPT: ¡Habla conmigo*. USA: Andreas Wnth, MSC.

LOS RIESGOS DE CORRUPCIÓN EN LA FASE DE EJECUCIÓN DE LA CONTRATACIÓN PÚBLICA

Y LOS CANALES INTERNOS Y EXTERNOS DE INFORMACIÓN Y LA PROTECCIÓN DEL INFORMANTE COMO MEDIO EFICAZ DE PROTECCIÓN DE LA INTEGRIDAD PÚBLICA



Joan A. Llinares
Director de la AVAF

En 2022 la Agencia Valenciana Antifraude publicó una recomendación con el objetivo de alertar sobre los riesgos en la ejecución de los contratos en clave de integridad pública¹. Una de las funciones previstas en la ley fundacional de la AVAF² es la de asesorar y formular propuestas en materia de cumplimiento de legalidad, ética pública y prevención de la corrupción dirigidas a los responsables de las entidades incluidas en su ámbito de actuación, incluyendo a todo el personal vinculado, indistintamente de si son cargos públicos o personal funcionario.

Estas recomendaciones, que además de remitirse a sus destinatarios institucionales se publican en la web de la Agencia³ para general conocimiento, constituyen a su vez un termómetro del grado de incumplimientos del ordenamiento jurídico detectados a través de otra función propia de la Agencia: las investigaciones de aquellos casos que se denuncian o se inician de oficio y que se refleja de forma muy detallada en las respectivas Memorias⁴ de la AVAF que se presentan anualmente al parlamento valenciano, Les Corts, en dación de cuentas de su actividad. En este sentido, es conveniente destacar que las administraciones públicas y sus entes vinculados, además del deber de ser transparentes, deben rendir cuentas y servir con objetividad los in-

tereses generales actuando con sometimiento pleno a la Ley y al Derecho⁵.



¹ Recomendación general "La ejecución de los contratos en clave de integridad pública" aprobada por Resolución de 27 de septiembre de 2022 del director de la AVAF.
² Ley 11/2016, de 28 de noviembre de la Agencia de Prevención y Lucha contra el Fraude y la Corrupción de la Comunitat Valenciana
³ <https://www.antifraucv.es/actuaciones-de-prevencion-2/>
⁴ <https://www.antifraucv.es/memorias-informes-y-dictamenes-2/>
⁵ CE art. 103.1 y exacciones ilegales. Arts. 436, 437 y 438 CP"

LA PREVENCIÓN DE LA CORRUPCIÓN EN LA EJECUCIÓN DE LOS CONTRATOS PÚBLICOS

Mediante la contratación pública las administraciones y sus entidades vinculan adquieren bienes, servicios y realizan obras públicas. También gestionan servicios públicos que se confían a empresas privadas a través de las concesiones. Mediante la contratación pública una buena parte de los impuestos de los contribuyentes retorna a la sociedad. En España, entre el 15 % y el 19 % del Producto Interior Bruto es aportado por las administraciones públicas a través de sus presupuestos anuales materializados en infinidad de contratos públicos. De los gestores públicos se espera que estas inversiones se lleven a cabo con altos estándares de eficacia, conductas éticas, cumplimiento de la legalidad y salvaguarda del interés general. Sin embargo, la Comisión Nacional de los Mercados y la Competencia (CNMC) cifró en un informe de 2017 que unos 40.000 millones de euros se pierden anualmente por fraude en la contratación pública generado principalmente por la ausencia de presión concurrencial y conductas colusorias como la de alterar el proceso competitivo, uno de cuyos casos dio lugar a una multa de 203,6 millones a 6 de las principales constructoras del país que durante más de 25 años habían estado concertándose para alterar las licitaciones de grandes obras de infraestructuras⁶. Hechos como estos nos ayudan a comprender mejor el sorprendente informe del Tribunal de Cuentas Europeo, de 2013, que advertía a la Comisión Europea que la construcción de una unidad de 1000m2 de autopista, excluidos los accidentes y factores orográficos, cuestan el doble en España que en Alemania. En aquel informe salieron tan mal parados como España otros dos países donde la corrupción es un problema grave: Grecia y Polonia.

No es de extrañar pues que la OCDE, en su informe de 2017 *"Integridad Pública, una estrategia contra la corrupción"*, sostuviera que entre un 10 y el 30 % de la inversión de un proyecto de construcción financiado con fondos públicos, puede malgastarse debido a la mala gestión y la corrupción.

Sin desdeñar obviamente las irregularidades que todavía se producen en el proceso de preparación y licitación de los contratos donde hay que reconocer que tanto las Directivas europeas sobre contratación pública, como la Ley 9/2017 de Contratos del Sector Público⁷,



han impactado positivamente al poner la corrupción como uno de los problemas a atajar, debemos destacar que una buena parte de los casos de fraude en los contratos públicos se produce en la fase de cumplimiento y ejecución del contrato.

Planteado el estado de la cuestión, se trata de que las administraciones públicas y sus entidades vinculadas establezcan planes antifraude⁸ en los procesos de ejecución de los contratos, extensible a las subcontrataciones y a cualquier forma de externalización financiada por fondos públicos o sufragadas por tasas o tarifas. En primer lugar, identificando y monitorizando los principales riesgos de corrupción durante la vida del contrato estableciendo las alertas (banderas rojas) sobre los comportamientos potencialmente nocivos más frecuentes en el día a día de la ejecución del contrato incluyendo los riesgos por ataques cibernéticos, fugas de información, el escaso control de cumplimiento de los clausulados sociales, ambientales o éticos, entre otros; enfatizando en la figura del responsable del contrato y estableciendo los mecanismos necesarios de prevención e integridad pública⁹.

Entre los riesgos generales citaremos los que siguen:

- Los derivados de la no detección, ocultación o falta de control de los

conflictos de interés reales, potenciales o aparentes.

- La ejecución de encargos o continuación de contratos finalizados sin título habilitante recurriendo torticeramente a la figura del enriquecimiento injusto.
- La ausencia o defectuosa planificación de la actividad contractual.
- La descoordinación entre las funciones de gestión y control del contrato.
- Ignorar la posible litigiosidad, responsabilidad patrimonial o civil.
- Falta de transparencia de los datos del contrato o su maquillaje para ocultar los déficits en la ejecución.

Entre los riesgos sectoriales destacamos los siguientes:

- Modificaciones del contrato sin estar previstas introduciendo prestaciones ajenas al objeto del contrato.
- Inejecución total o parcial de mejoras o variantes que formarían parte de la oferta adjudicada pero que no se exige su cumplimiento.

- Prórrogas imprevistas de los contratos alterando su duración más allá de lo previsto.
- Pagos irregulares o injustificados que no se corresponden con el objeto del contrato.
- Pagos de servicios no realizados, en ocasiones encubiertos en las facturas o certificaciones entre los que sí se realizan.
- Ausencia de control en los cambios en la persona del contratista tales como cesiones del contrato en terceros que no reúnen las condiciones exigibles.
- Subcontrataciones no autorizadas en terceras empresas.
- Ausencia de exigencia de responsabilidades por incumplimiento del contrato.
- Abuso del contrato menor para eludir la publicidad y concurrencia.
- Simulación de la concurrencia competitiva aportando ofertas de diversas empresas pero que en realidad tienen los mismos titulares.
- La huida de los procedimientos de contratación a través de supuestos convenios de colaboración.
- Extinción de los contratos por causas no previstas sin exigencia de responsabilidades.
- Liquidación de las obligaciones sin ajustarse a las condiciones del contrato.
- Ausencia de reacción cuando el contratista incumple las condiciones retributivas, convenios colectivos, planes de igualdad, etc. en perjuicio de sus trabajadores.

Y por último estarían los riesgos que se derivan de la insuficiencia o inadecuado control interno; la ausencia de la comprobación material de la ejecución del contrato, omisión de la fiscalización o de auditoría analítica, y en casos de alarmas sospechosas, auditoría forense.

LOS CANALES INTERNOS Y EXTERNOS Y LA PROTECCIÓN DE LOS INFORMANTES DE CONDUCTAS CORRUPTAS O CONTRARIAS A LA INTEGRIDAD PÚBLICA

No podemos ignorar que gran parte de los fraudes que se producen en la contratación pública, especialmente en la fase de ejecución, son difíciles de detectar llegando a conocimiento de instituciones como la AVAF gracias en gran medida a la colaboración de aquellas personas que por su cercanía con el contrato son conocedores de las irregularidades e incumplimientos y se deciden a informar a las autoridades u órganos de control. En demasiadas ocasiones estas personas sufren represalias a pesar de que están defendiendo la legalidad.

Precisamente, para evitar estas represalias y facilitar las denuncias de las infracciones de la legalidad en el ámbito de las administraciones públicas, otra de las funciones de la AVAF es la de proteger a los denunciantes contra esas posibles represalias. Desde 2017, año de inicio de la actividad, han sido 34 personas físicas y una persona jurídica las que han recibido el amparo y protección de la Agencia consistente en asesorar jurídicamente a las personas informantes garantizando la confidencialidad de su identidad y, en los casos donde el riesgo de represalias lo aconseja, otorgar el **estatuto de persona denunciante** considerando persona denunciante a cualquier persona física o jurídica que comunique hechos que pueden dar lugar a la exigencia de responsabilidades legales¹⁰.

Para facilitar las denuncias, desde el año 2018 la AVAF estableció procedimientos y canales confidenciales¹¹ incluso con la posibilidad de guardar el anonimato, utilizando la tecnología Globaleak¹², un canal de sencillo manejo accesible desde la web de la AVAF y que desde 2015 estaba en funcionamiento en el Ayuntamiento de Barcelona gestionado por su órgano anticorrupción denominado Oficina de Transparencia y Buenas Prácticas¹³ que en aquella época tuvo el honor de dirigir.

Por este canal electrónico entran en la AVAF casi el 90 por 100 de las denuncias relativas a irregularidades en la contratación pública, pero también sobre irregularidades en la gestión de recursos humanos; el manejo de fondos públicos; la gestión urbanística; la concesión o aplicación de subvenciones; la gestión de patrimonio público; etc.

La AVAF tiene el deber de velar por que las personas que denuncian no sufran, durante la investigación, ni después de ella, ningún tipo de persecución, aislamiento o empeoramiento de las condiciones laborales o profesionales,

ni ningún tipo de medida que implique cualquier forma de perjuicio o discriminación. Esta protección puede extenderse, en su caso, al cónyuge o persona a quien se encuentre ligado por análoga relación de afectividad o a los ascendentes, descendientes o hermanos.

Para poder hacer efectiva esta función protectora, la Agencia tiene potestad sancionadora y su ley tipifica las conductas represaliadoras como infracciones muy graves que pueden ser penalizadas con multas de 30.000 a 400.000 euros además de considerar nulos de pleno derecho cualquier acto o resolución adoptadas como base de conductas corruptas o fraudulentas tipificadas en la ley¹⁴. La citada ley fundacional considera responsables de las infracciones, incluso a título de simple inobservancia, las personas físicas o jurídicas, cualquiera que sea su naturaleza, las autoridades, directivos, y el personal al servicio de las entidades previstas en la ley, que realicen acciones o que incurran en las omisiones en ella tipificadas bien sea con dolo, con culpa o con negligencia.

Años después de estar vigente en la Comunitat Valenciana la ley 11/2016 de la AVAF se aprobó por el Parlamento de España 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 corrupción¹⁵, como trasposición de la Directiva UE 2019/1937 conocida como *"Directiva Whistleblowers"*. A través de esta ley todas las administraciones públicas y sus entes vinculados, así como las empresas del sector privado con más de 50 trabajadores, están obligadas a tener activo un sistema de información interno que canalice las denuncias y a su vez estar conectadas con el canal de denuncias que gestiona la autoridad externa, sea la estatal o la autonómica.

Asimismo, la Ley 2/2023 también prohíbe, como ya lo anticipó la ley fun-

¹⁰ Artículo 14 de la Ley 11/2016, de la AVAF 41 y ss. de su Reglamento. ⁷ El artículo 64 de la LCSP hace referencia expresa, por primera vez en una ley de contratos públicos, a la lucha contra la corrupción y prevención de los conflictos de interés.

¹¹ Buzón de denuncias y oficina virtual del empleado público https://www.anti frau cv.es/wp-content/uploads/2021/03/2018_4529.pdf

¹² Tecnología open source de canal de denuncias <https://www.globaleaks.org/features/#technical-features>

¹³ Bústaia Ética Ajuntament de Barcelona <https://ajuntament.barcelona.cat/premsa/2015/11/26/barcelona-crea-loficina-per-la-transparencia-i-les-bones-practiques/>

¹⁴ Artículo 17 y ss. de la Ley 11/2016 de la AVAF.

¹⁵ Ley 2/2023 reguladora de la protección de las personas informantes y de lucha contra la corrupción <https://www.boe.es/buscar/act.php?id=BOE-A-2023-4513>

⁶ <https://www.cnmc.es/prensa/sancionador-obra-civil-20220707>

⁷ El artículo 64 de la LCSP hace referencia expresa, por primera vez en una ley de contratos públicos, a la lucha contra la corrupción y prevención de los conflictos de interés.

⁸ Guía de la AVAF para elaborar planes de integridad

⁹ Ver el catálogo de riesgos contrarios a la integridad pública en materia de contratación pública https://www.anti frau cv.es/wp-content/uploads/2023/09/WEB_v2-Catalogo-de-Riesgos-Contratacion.pdf



dacional de la AVAF siete años antes, cualquier acto o conducta que pudiera considerarse una represalia contra la persona que informe o comunique infracciones del ordenamiento jurídico estableciendo fuertes sanciones para los represaliadores y declarando como actos nulos de pleno derecho las decisiones consideradas represalias.

Pendientes en el momento de escribir estas líneas, del nombramiento de la Autoridad Nacional Independiente de Protección, el órgano creado por la co-

mentada ley estatal para velar por la protección de los "Whistleblowers" y canalizar las denuncias que afectan a la administración del Estado o al resto de administraciones públicas y empresas del sector privado en los territorios que no existan autoridades autonómicas que tengan atribuidas por ley estas competencias, en ámbito público de la Comunidad valenciana es la AVAF la autoridad protectora y la responsable del sistema externo de denuncias para todo el sector público por así reconocerlo expresamente la Ley 2/2023.

Además, el apoyo de la AVAF a todo el sector público valenciano se materializa en la ayuda y asesoramiento a todas las administraciones valencianas para la puesta en funcionamiento de los canales internos de denuncias facilitando gratuitamente la tecnología estandarizada, homologada por la Comisión Europea, y ayudando a instalarla y formando a sus con un objetivo general: la construcción de una sólida red de integridad de todas las administraciones públicas y sus entidades vinculadas que actúe como dique contra las conductas corruptas.

QUÉ DEBEMOS TENER EN CUENTA PARA HACER NEGOCIOS EN LATINOAMÉRICA DESDE LA PERSPECTIVA DEL COMPLIANCE OFFICER



Fernando Peyretti
Socio de Forensics Deloitte Spanish Latam

América Latina tiene un escenario de delitos financieros muy desafiante. En ella se identifican, principalmente, las siguientes actividades ilícitas: contrabando de minerales, tráfico de drogas, trata de personas (que también incluye el tráfico ilícito de migrantes)¹, actividades que a su vez están generando flujos de efectivo ilegales relacionados con los Delitos Financieros más típicos de la región, tales como: Lavado de Activos (LA), Lavado de Activos Basado en el Comercio (LABC), Financiamiento del Terrorismo (FT), Corrupción, y Fraude Corporativo.

En referencia a las actividades ilícitas analizadas, es posible detallar lo siguiente:

El contrabando de minerales o la minería ilegal incluye, según la definición de la Comisión de Prevención del Delito y Justicia Penal², "el tráfico de metales preciosos extraídos ilegalmente, y las actividades ilegales de explotación de recursos minerales realizadas por grupos delictivos organizados". Según la OCDE, uno de cada cinco casos de corrupción transnacional ocurre en el sector extractivo. Además, Latinoamérica es reconocida como exportadora (ilegal), principalmente a Estados Unidos, Europa y Asia, siendo el oro el artículo más extendido dentro de los metales preciosos comercializados ilegalmente.

Si nos centramos en el contrabando de

minerales, existen en la región gran diversidad de regulaciones locales con diferentes enfoques y algunas iniciativas globales como la Iniciativa para la Transparencia de las Industrias Extractivas (EITI)³. De acuerdo con las prioridades estratégicas del EITI, existen programas como la Alianza para las Contrataciones Abiertas que se están aplicando en Argentina, Colombia, Ecuador, Guatemala, México, Nicaragua, Perú, República Dominicana y Surinam que ponen a disposición de los ciudadanos información de libre acceso⁴.

En cuanto al tráfico de drogas, evaluando las estimaciones de la Oficina de



¹ Financial Crime in Latin America and the Caribbean: Understanding Country Challenges and Designing Effective Technical Responses, octubre de 2021, disponible en: <https://gfintegrity.org/report/financial-crime-in-lat-in-america-and-the-caribbean/>

² La CCPCJ es el órgano preparatorio de los Congresos de las Naciones Unidas sobre Prevención del Delito y Justicia Penal. Las declaraciones adoptadas durante los congresos se transmiten mediante la CCPCJ y el ECOSOC a la Asamblea General para su aprobación.

³ La misión de la Iniciativa para la Transparencia de las Industrias Extractivas (EITI, por sus siglas en inglés) es promover el conocimiento sobre la gestión de los recursos naturales, fortalecer la gobernanza y la rendición de cuentas en las esferas pública y corporativa, y proporcionar datos que sirvan de base para la creación de políticas y el diálogo entre múltiples partes interesadas en el sector extractivo.

⁴ Informe de Progreso EITI 2022, junio de 2022, disponible en: <https://eiti.org/documents/eiti-progress-report-2022>

las Naciones Unidas contra la Droga y el Delito (UNODC)⁵, las incautaciones se están llevando a cabo cada vez más cerca de los sitios de producción en América del Sur (principalmente de Colombia, Bolivia y Perú), donde la cantidad total incautada es ahora tres veces mayor que en América del Norte.

Por lo que respecta a la trata de personas, qué, según el Protocolo contra la trata de personas de la Oficina de las Naciones Unidas contra la Droga y el Delito, se define como "la captación, el transporte, el traslado, la acogida o la recepción de personas por la fuerza, el fraude o el engaño, con el fin de explotarlas con fines de lucro", la UNODC estima el valor del tráfico ilícito de migrantes en una cifra de entre 3.700 y 4.200 millones de dólares al año⁶. Estados Unidos es uno de los principales destinos de los migrantes ilegales de América Latina.

Los Delitos Financieros asociados a las Actividades Ilícitas anteriormente descritas se destacan por lo siguiente:

1. BLANQUEO DE CAPITAL

La Convención de Viena describe el blanqueo de dinero como: "convertir o transferir a sabiendas bienes derivados de cualquier delito para ocultar o disfrazar el origen ilícito de los mismos, o ayudar a cualquier persona involucrada en dicho delito o delitos a evadir las consecuencias jurídicas de sus actos. Y según el Instituto de Gobernanza de Basilea (BIS⁷, por sus siglas en inglés), las principales deficiencias son los bajos niveles de transparencia financiera y de rendición de cuentas. Todos los países de América Latina, excepto tres (Chile, Uruguay, y Granada), están incluidos en la lista de las principales jurisdicciones de lavado de dinero en el INCSR del Departamento de Estado de EE. UU. de este año⁸.

2. BLANQUEO DE CAPITAL BASADO EN EL COMERCIO (TBML)

El GAFI lo define como "el proceso de ocultar el producto del delito y mover va-

lores mediante el uso de transacciones comerciales, en un intento de legitimar su origen ilegal o financiar sus actividades. Las recomendaciones del GAFI para la región latinoamericana implican un fuerte avance en la promulgación de leyes que permitan a los países combatir este tipo de delitos de manera efectiva.

3. FINANCIACIÓN DEL TERRORISMO

Como se establece en el Convenio Internacional para la represión de la financiación del terrorismo de las Naciones Unidas⁹, que define la financiación del terrorismo como el suministro o la recaudación de fondos, "por cualquier medio, directa o indirectamente, ilegal y deliberadamente, con la intención de ser utilizados o de ser utilizados a sabiendas para actos de terrorismo". La financiación del terrorismo es un tipo de delito financiero que también puede superar a otros como el blanqueo de capitales y la corrupción. En este caso, el elemento distintivo no es el origen ilícito del fondo, sino la finalidad del uso de los fondos. Los casos más relevantes son:

Los grupos terroristas nacionales designados en los países de América Latina y el Caribe incluyen al ELN (Colombia), las Disidencias de las FARC (Colombia) y Sendero Luminoso (Perú) son hoy más pequeños, en comparación con la magnitud que tenían en el pasado.

Desde 2007 se han registrado un total de 33 muertes por terrorismo en Centroamérica y el Caribe, de las cuales el 24% ocurrieron en 2009. La región no ha registrado muertes por terrorismo desde 2018, sin embargo, ha sufrido mucho a causa de otras formas de conflicto violento, sobre todo un aumento de los homicidios asociados con la delincuencia organizada y la violencia relacionada con las drogas¹⁰.

Los riesgos de Financiación del Terrorismo se extienden más allá de la actividad de terrorismo nacional, e incluyen casos de ser utilizados como punto de tránsito o área de preparación para el terrorismo

en otros lugares.

4. CORRUPCIÓN

El GAFI ha destacado en repetidas ocasiones que la corrupción "florece en un entorno en el que los funcionarios del Estado y los empleados del sector público abusan de sus cargos para obtener beneficios privados".

Según el *Índice de Percepción de la Corrupción 2022* elaborado por Transparencia Internacional, "por cuarto año consecutivo, las Américas obtienen una puntuación promedio de 43 sobre 100¹². La falta de medidas audaces y decisivas para luchar contra la corrupción y fortalecer las instituciones públicas está

¹¹ Actualmente son miembros de las Naciones Unidas 193 Estados, que están representados en el órgano deliberativo, la Asamblea General, el principal foro mundial donde todas las naciones del mundo pueden reunirse y encontrar soluciones compartidas que beneficien a toda la humanidad.

¹² Índice de Percepción de la Corrupción 2022, enero de 2023, disponible en: <https://www.transparency.org/en/publications/corruption-perceptions-index-2022>



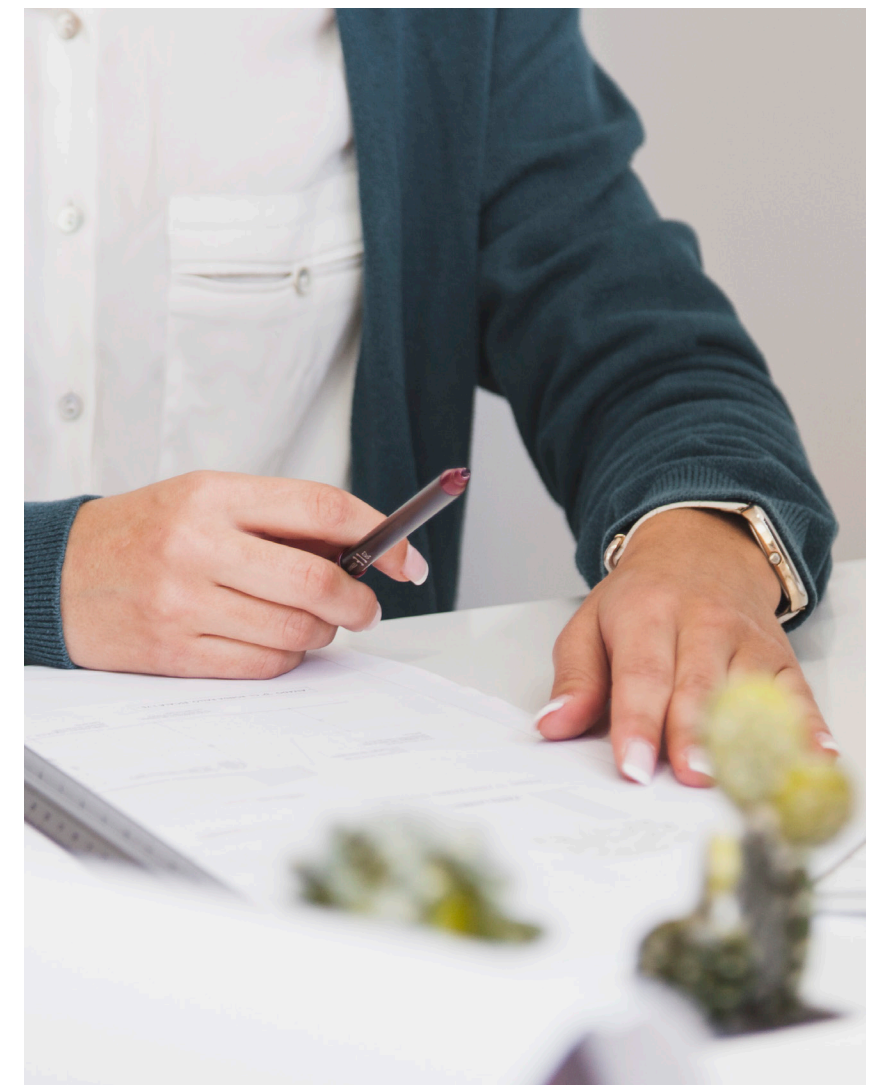
alimentando las actividades de la delincuencia organizada y otras fuentes de violencia. También está socavando la democracia, los derechos humanos y el desarrollo; y según el *Barómetro Global de la Corrupción para América Latina y el Caribe 2019*¹³. La corrupción contribuye a la erosión de la confianza de los ciudadanos en el gobierno. Los resultados muestran que la confianza en los gobiernos, los tribunales, y la policía es muy baja en América Latina y el Caribe. La corrupción prevalece en la mayoría de los aspectos ordinarios de la vida cotidiana, incluida, entre otras cosas, la corrupción a gran escala en el sector público y privado, que afecta a la vida de los ciudadanos de a pie. Según Transparencia Internacional, 56 millones de personas entre los 18 países de América Latina y el Caribe pagaron sobornos en 2018.

5. FRAUDE CORPORATIVO

Según la ACFE¹⁴, hay tres categorías principales de fraude ocupacional. La apropiación indebida de activos, que implica la sustracción ilegal, o el mal uso de los recursos del empleador, es la más común, con un 86% de los casos que entran en esta categoría. Sin embargo, esta tipología tiende a causar la pérdida promedio más baja, siendo de 100.000 dólares por caso. Por el contrario, los esquemas de fraude a los estados financieros, en los que el perpetrador, intencionalmente, induce a un error u omisión material en los estados financieros de la organización, es la categoría más inusual (9% de los esquemas fraudulentos identificados) pero, en promedio, la más costosa (USD 593,000 por caso). La tercera categoría, denominada "corrupción", que incluye delitos como el soborno, los conflictos de intereses y la extorsión, se encuentra en el medio de las anteriores dos, en términos de frecuencia y pérdidas. Estos esquemas ocurren en el 50% de los casos y causan una pérdida media de USD 150.000¹⁵. Es importante tener en cuenta que las 3 tipologías señaladas, a menudo ocurren de forma concurrente.

Además, las organizaciones, en promedio, pierden el 5% de sus ingresos debido a esquemas de fraude anualmente. Se estima que cada año se pierden 4,7 billones de dólares debido al fraude en todo el mundo.

Los asuntos abordados anteriormente permiten comprender la existencia de numerosos casos de fraude y corrupción público-privada que involucran y



afectan tanto a las empresas como a los propios Estados de la región.

Exploremos los resultados de un caso muy conocido. Odebrecht fue objeto de la mayor sanción económica aplicada por Estados Unidos, en relación con la FCPA, que asciende a 3.560 millones de dólares. La investigación incluye sobornos a funcionarios públicos durante el período comprendido entre 2001 y 2016. Una conclusión relevante es que el monto total de los pagos por sobornos identificados ascendió a US\$788 millones, y el total de las utilidades obtenidas, o gastos evitados, producto de estos, ascendió a US\$3.336 millones. Así, la relación entre la sanción y los sobornos pagados es de 451,89% (US\$3.560.868.772 / US\$788.000.000), y la relación entre la sanción y la ganancia obtenida derivada de los sobornos pagados es de 106,74% (\$3.560.868.772 / \$3.336.000.000). Es un mensaje contundente de los reguladores, que indica que la corrupción no es un negocio rentable, y esto es un incentivo clave, junto con las distintas regulaciones para la lucha contra la co-

rrupción que se sancionaron en América Latina para fortalecer la implementación de Programas de Integridad por parte de las organizaciones¹⁶.

De acuerdo con las estadísticas oficiales, el período más significativo en la aplicación de las sanciones de la FCPA comenzó en 2008, con un monto total de sanciones en el período que abarca desde 2008 hasta la actualidad, que representa US\$ 29 mil millones en comparación con los 30 años anteriores, lo que implicó un total de sanciones acumuladas que ascendieron a solo US\$ 408 millones entre 1977 y 2007¹⁷. Además, este período de fuerte crecimiento de las sanciones coincide con la publicación de las "Recommendation of the Council for Further Combating Bribery of Foreign Public Officials in International Business Transactions" por parte de la OCDE en¹⁸ 2009. Es posible identificar que la normativa anticorrupción se aplicó siguiendo las recomendaciones de la OCDE en los siguientes países de América Latina: Chile, Brasil, México, Colombia, Perú, Argentina, Ecuador, Costa

⁵ La Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC) es líder mundial en la lucha contra las drogas ilícitas y el crimen internacional, además de estar a cargo de ejecutar el principal programa de las Naciones Unidas contra el terrorismo.

⁶ Estudio mundial sobre el tráfico ilícito de migrantes, junio de 2018, disponible en: <https://www.unodc.org/unodc/en/data-and-analysis/glossom.html>

⁷ Es una organización independiente sin fines de lucro dedicada a luchar contra la corrupción y otros delitos financieros y a mejorar los estándares de gobernanza. El BIS está registrado como una fundación suiza y es un Instituto Asociado de la Universidad de Basilea.

⁸ Índice AML de Basilea 2023: 12ª edición pública que clasifica los riesgos de blanqueo de capitales y financiación del terrorismo en todo el mundo, noviembre de 2023, disponible en: <https://baselgovernance.org/basel-aml-index>

⁹ Actualmente son miembros de las Naciones Unidas 193 Estados, que están representados en el órgano deliberativo, la Asamblea General, el principal foro mundial donde todas las naciones del mundo pueden reunirse y encontrar soluciones compartidas que beneficien a toda la humanidad.

¹⁰ Índice Global de Terrorismo 2022, mayo de 2022, disponible en: <https://www.economicsandpeace.org/reports/>



Rica y Bolivia.

El actual entorno de negocios de América Latina y el Caribe plantea un alto riesgo de corrupción que las empresas deben evaluar con especial atención, considerando las particularidades de cada uno de los países.

Desde el punto de vista de la evolución de las regulaciones para combatir los delitos financieros, y la efectividad de los mecanismos actuales contra el Lavado de Activos y el Financiamiento del Terrorismo en la región, la región de América Latina es un punto de origen, tránsito y destino en las etapas de colocación, estratificación e integración del lavado de activos. El dinero ilícito se envía desde la región y se recibe dentro de la región.

Complementando esto con el Índice Basil AML, existe una importante heterogeneidad en la región, evidenciada por las diferentes capacidades institucionales de cada uno de los países para mitigar los riesgos asociados al lavado de activos y al financiamiento del terrorismo.

Solo 8 países de América Latina, tales como: Argentina, Brasil, Colombia, Costa Rica, Ecuador, Panamá, Perú, Paraguay, República Dominicana y Uruguay cuentan con un registro de beneficiarios finales¹⁹.

Recomendaciones clave:

- Un claro apoyo desde la alta dirección: será fundamental para navegar los desafíos en materia de Compliance que nos presenta la región de Latinoamérica, que la lucha contra el fraude y la corrupción ocupe un lugar relevante dentro de la estrategia de las organizaciones.
- Identificación de riesgos: Comprender como impactan los riesgos mencionados previamente en todos los procesos de negocios de la compañía. La identificación de riesgos como punto de partida es central para desarrollar esquemas de control interno adaptados a cada organización, y al entorno donde esta desarrolla sus actividades.
- Monitoreo y evaluación continua: Es fundamental que las organizaciones aumenten sus inversiones en tecnología para robustecer los ambientes de control interno, en escenarios en los que la transformación digital y la aplicación de inteligencia artificial a los procesos de negocios continuará expandiéndose.
- Identificación de debilidades de Ciberseguridad: Durante el período posterior a la pandemia, las organizaciones tomaron mayor conciencia respecto la importancia de llevar adelante una estrategia de digitalización de los negocios, en los que la ciberseguridad tenga un rol protagónico, a la luz de las experiencias ocurridas durante los años de pandemia, en el que se identificó un aumento exponencial de los esquemas fraude basados

en debilidades de ciberseguridad.

- Capacitación a los empleados y a terceras partes: Las organizaciones deben realizar capacitaciones periódicas tanto a los empleados, como parte de sus programas antifraude y anticorrupción, e incluir al personal clave, vinculado a servicios estratégicos provistos por terceros.
- Due Diligence de Integridad: Más de 95% de las investigaciones que implicaron sanciones en el marco de la FCPA demostraron la participación de terceras partes en el desarrollo de esquemas de pagos de sobornos a funcionarios públicos, es fundamental que las organizaciones comprendan con profundidad con quienes interactúan a la hora de hacer negocios.
- Investigaciones internas: Las decisiones de la SEC y el DOJ han demostrado que pueden ocurrir graves efectos negativos en la capacidad de operación de una organización si no siguen los métodos adecuados de recopilación de evidencias y aprovechamiento del análisis de datos para analizar de manera eficiente grandes conjuntos de datos. Al ejecutar estos procedimientos, los mundos legales y financieros están entrelazados y, en muchos casos, requieren colaboración para resolver disputas legales complejas, cuestiones regulatorias e investigaciones. Es fundamental para las empresas buscar la complementación de sus equipos legales, sus asesores legales externos, y los equipos de contadores forenses que participen en las investigaciones para lograr resultados óptimos. Los contadores forenses pueden brindar asistencia valiosa a las firmas de abogados de diversas maneras, como analizando datos financieros para detectar y prevenir actividades fraudulentas,

identificando señales de alerta financieras, y garantizando el cumplimiento normativo.

Aprovechando su experiencia en técnicas de contabilidad e investigación, los contadores forenses pueden ayudar a los abogados con la diligencia debida de integridad, el cumplimiento normativo, la prevención del fraude, el análisis informático forense, y la ejecución de testeos de transacciones para identificar señales de alerta financieras, entre otros²⁰.

- Implementación de canales de denuncia: A nivel internacional el 42% de los casos se detectan por esta vía, siendo la principal herramienta de detección de casos de fraude. Es deseable que las organizaciones rápidamente implementen canales que aseguren la

confidencialidad y el anonimato, acompañados por políticas anti represalias, para garantizar la protección de los denunciantes de buena fe.

- Fortalecimiento de la función de Compliance: Durante los últimos años, vimos como cada vez más compañías incorporaron roles de Compliance, y desarrollaron sus programas de Integridad, en paralelo con la promulgación de normas anticorrupción promovidas por la OCDE en muchos países de Latinoamérica, así como por el fuerte *enforcement* de la FCPA. Las empresas deben profundizar esta tendencia, incorporando el Compliance como parte central de la estrategia de negocios, y llevando los programas de Compliance a un siguiente nivel de madurez.

¹⁹ El estado actual de los registros de beneficiarios finales en América Latina, Tax Justice Network, marzo de 2023, Disponible en: <https://taxjustice.net/2023/03/17/transparencia-de-beneficiarios-finales-en-america-latina-avances-pero-aun-queda-mas-por-hacer>

²⁰ Lexis Nexis, The Guide to Corporate Compliance - Fourth Edition: It Takes Two to Tango: How Forensic Accountants Can Complement Attorneys. Disponible en: <https://latinlawyer.com/guide/the-guide-corporate-compliance/fourth-edition/article/it-takes-two-tango-how-forensic-accountants-can-complement-attorneys#:~:text=While%20attorneys%20and%20forensic%20accountants,specific%20needs%20of%20an%20organisation>



¹³ Barómetro Global de la Corrupción para América Latina y el Caribe 2019, septiembre de 2019, disponible en: <https://www.transparency.org/en/gcb/latin-america/latin-america-and-the-caribbean-x-edition-2019>

¹⁴ La Asociación de Examinadores de Fraude Certificados (ACFE, por sus siglas en inglés) es una de las organizaciones antifraude más grandes del mundo. Ofrece la credencial CFE, una de las más reconocidas internacionalmente entre los profesionales antifraude.

¹⁵ Informe ACFE 2022 a las Naciones, disponible en: <https://legacy.acfe.com/report-to-the-nations/2022/>

¹⁶ Facultad de Derecho de Stanford, disponible en: <https://fcpa.stanford.edu/enforcement-action.html?id=635>

¹⁷ Facultad de Derecho de Stanford, disponible en: <https://fcpa.stanford.edu/statistics-analytics.html?tab=2>

¹⁸ La Organización para la Cooperación y el Desarrollo Económicos (OCDE) es una organización internacional cuya misión es diseñar mejores políticas para una vida mejor. La OCDE es un foro único, un centro de conocimiento para la recopilación y el análisis de datos, el intercambio de experiencias y buenas prácticas, que, en colaboración con los gobiernos, trabaja para establecer estándares internacionales y proponer soluciones para diversos desafíos sociales, económicos y sociales y ambientales.

LA ESTANDARIZACIÓN DE LOS PROCESOS DE INVESTIGACIÓN. DE LA TEORÍA A LA METODOLOGÍA



Leocadio Marrero Trujillo

L.A. ISO 27001+27017+27701+22301

L.I. ISO 27001 e ISO 22301

L.I. ISO 37301 Compliance

DPO-Data Protection Officer

CDPSE.ISACA

Un viaje a través del nuevo estándar internacional establecido por ISO.org bajo el nombre **ISO/TS 37008:2023 Investigaciones Internas de Organizaciones: Orientación.**

Define el RAE la investigación como la “acción y efecto de investigar”. Este concepto tiene su origen en el latín ‘investigare’, un término que, a su vez, proviene del vocablo ‘vestigium’, que viene a tener una interpretación como “pos de la huella de”, algo así como, volver sobre la marca que ha dejado la suela del pie, para ir tras la búsqueda de esa huella o vestigio².

Desde un punto de vista técnico, podría referirnos a ella como “el proceso mediante el cual se adquiere conocimiento. Por lo tanto, tiene como objetivo la adquisición de conocimientos nuevos, la ampliación de otros existentes o la solución de problemas teóricos o prácticos por medio de una actividad metódica y reproducible³”. Un aspecto en el que también, Luz Leherer caracteriza la investigación, es decir, ‘aplicando un método determinado, siguiendo pasos de modo ordenado y sistemático’.

Es en el propio glosario de términos y definiciones de la cláusula 3, bajo el epígrafe 3.1 Investigación Interna, que la propia norma ISO 37008 define esta actividad como ‘Proceso profesional de investigación de hechos, iniciado por o para una organización, para establecer hechos en relación con presuntas sospe-

chas de irregularidades, mala conducta o incumplimiento⁴’. Y, bajo el epígrafe 3.14 la norma UNE/ISO 37002:2021 de Sistema de Gestión de la denuncia de irregularidades, la refiere como “Proceso sistemático, independiente y documentado para establecer los hechos y evaluarlos objetivamente para determinar si hubo irregularidades, están ocurriendo o es probable que ocurran y su alcance⁵”.

En el ecosistema internacional existen normas o estándares para ejecutar esta actividad de forma ordenada, metodológica y profesional. Por poner un ejemplo, está AGIS⁶ (Estándar de Investigaciones del Gobierno Australiano), con un claro ámbito de afectación territorial que, como bien señalamos, pretende ordenar de forma profesional, metodológica y, muy importante, de forma repetible, la difícil encomienda de la investigación interna, que entró en vigor el 31 de octubre de 2022.

Desde el punto de vista del Compliance, las investigaciones internas son una característica de los programas de cumplimiento, que cada vez cobran más vigencia, impulsados por la proliferación de leyes, regulaciones y estándares. Por poner un claro ejemplo, solo tenemos que echar un vistazo a la Directiva

2019/1937 de Protección al Informante⁷, de ha dado lugar, en el caso español, a las transposición de la norma 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 corrupción⁸, que en el artículo 19 refiere a esta actividad bajo el término ‘Instrucción’, señalando que la misma ‘comprenderá todas aquellas actuaciones encaminadas a comprobar la verosimilitud de los hechos relatados’. Todo esto impulsó a la organización ISO ha trabajar en el desarrollo y posterior publicación del estándar ISO 37008, el pasado mes de julio del 2023.

A continuación, haremos y contextualizaremos los aspectos más relevantes que trae consigo esta norma internacional, especialmente los elementos que suministrarían la base para la gestión de la misma, dejando fuera de este artículo el Anexo A de la misma.

¿QUÉ APORTA ISO 37008 A LOS PROCESOS DE INVESTIGACIÓN?

Como estándar, no solo se esfuerza por enunciar los principios que deben inspirar esta actividad interna en las organizaciones, sino que viene a dotarle de un elemento motriz gerencial estratégi-

co, como son las políticas y la definición de los procedimientos de marcado carácter garantista, clave para la función de Gobierno por parte de las organizaciones afectadas.

Con ese apoyo, la labor investigadora se sustentará en un conjunto de principios (Cláusula 4) que deberá dar equilibrio y sustento a la actividad y que la va a caracterizar. Estos principios son:

- 4.1 Independencia
- 4.2 Confidencialidad
- 4.3 Objetividad e imparcialidad
- 4.4 Competencia y profesionalidad
- 4.5 Legalidad y licitud

Elementos garantes de la función de gobierno, son que el Órgano de Gobierno deberá (Cláusula 5):

1.- Apoyar el establecimiento, implementación, mantenimiento y mejora continua de las investigaciones interna, lo que incluirá la política o el procedimiento de ejecución de las investigaciones.

2.- Deberá proporcionar los recursos necesarios, entre ellos: personal, financiero, técnicos y organizativos, pudiendo estos recursos ser internos o externos.

Por tanto, el Órgano de Gobierno deberá demostrar el liderazgo y compromiso, a la vez que deberá estar ‘razonablemente informados’ en consonancia con el plan de comunicación establecido para esta función investigadora, garantizando que la información solo se comparta con las personas que tienen la ‘necesidad’ de saber, según el procedimiento escrito y que deberá responder a principios de ejecución como el de minimización de datos y el de mínimo privilegio, para garantizar la confidencialidad, segundo de los principios en juego.

En el plano operativo y práctico de la ejecución de la tarea de investigación (Cláusula 7) tiene que ver con la preservación y protección de las pruebas objeto de la actividad investigadora. Probablemente estemos ante una de las actividades más delicadas, de ahí que el 4º de los principios, exija competencia y profesionalidad en su desempeño. ¿Por qué? Porque la labor investigadora deberá contemplar dos planos:

1.- EL FONDO:

- Identificar dónde se pueden encontrar las pruebas o evidencias pertinentes.



- Determinar el riesgo de que algún investigado pueda abandonar la organización.
- Evitar que se manipule a los testigos y se borren, destruyan o alteren las pruebas.
- Garantizar la custodia de las pruebas y que las mismas no sean accedidas por personas no autorizadas a ello.

2.- EL FORMAL:

- Garantizar que la actividad de investigación si lleve a cabo sin amenazas, promesas, incentivos u opresión; que se hagan de forma discreta, respetando la privacidad y salvaguardando la confidencialidad de las pruebas aportados por los testigos.
- Definir y adoptar medidas para evitar represalias en cualquiera de sus formas: presión, intimidación, amenaza, acoso, etc...
- Garantizar la salvaguardia el bienestar físico y psicológico de quienes participen del proceso investigador.

Sin duda, ambos planos, el de fondo y el formal, representan un auténtico desafío para que las organizaciones puedan llevar cabo esta actividad, no olvidemos que el factor humano contribuye, inexorablemente, a generar inestabilidad y puede influir, ya sea de palabra o de obra (pensemos en el poder del lenguaje corporal), en otro de los principios, el tercero, que la norma enarbolaba, la objetividad e imparcialidad.

¿Cómo se debe llevar a cabo del proceso de investigación encomendado por el Órgano de Gobierno?

Es aquí donde la política o procedimiento deberá contar con una matriz RACI que establezca y fije los roles que van a intervenir, con qué función y en qué actividades propias de la investigación.

Pues bien, la primera de las decisiones del Órgano de Gobierno es el establecimiento de una ‘línea jerárquica’ que debe ser la responsable de aplicar sanciones y recomendar actuaciones adicionales de seguimiento de la investigación (salidas).

Para poder ejecutar esas acciones, la línea jerárquica debe contar con una serie de elementos (entradas) que sumi-

¹ RAE.

² Por LUZ LEHERER: <https://definicion.com/investigacion/>

³ <https://economipedia.com/definiciones/investigacion.html>

⁴ ISO/TS 37008:2023 3.1 Investigación Interna.

⁵ UNE ISO 37002:2021 Sistema de Gestión de la denuncia de irregularidades

⁶ <https://www.afp.gov.au/sites/default/files/PDF/Australian-Government-Investigations-Standard-2022.pdf>

⁷ <https://www.boe.es/doue/2019/305/L00017-00056.pdf>

⁸ <https://www.boe.es/buscar/act.php?id=BOE-A-2023-4513>



nistren la materia prima que ayude, para lo cual el equipo de investigadores deberá reportar de forma periódica o a intervalos planificados, según el plan de comunicación, y presentar informes para su revisión.

¿Qué implicaciones conlleva la actividad de la línea jerárquica? Por ejemplo, conllevaría:

- Evaluación de la naturaleza de las acusaciones.
- Verificar la inexistencia de conflicto de interés (ISO 37001, en la cláusula 3.29 lo define como *"situación donde los intereses de negocios, financieros, familiares, políticos o personales podrían interferir con el juicio de valor del personal en el desempeño de sus obligaciones hacia la organización"*).
- Revisar futuras interacciones con las autoridades y otras partes interesadas.
- Evaluar la gravedad del problema objeto de investigación.
- Evaluar, en términos de impacto, el riesgo financiero, reputacional o regulatorio implicado en la acción.

Mientras tanto, el equipo investigador deberá esforzarse por realizar una evaluación preliminar del problema; es decir, ver la naturaleza y credibilidad del hecho denunciado, comunicarse con el denunciante (siempre que sea posible) y solicitar información adicional y, documentar el informe; desde ahí, determinar si el equipo actual es competente en número y especialidad para hacer frente al encargo de la investigación.

Con este informe preliminar (entrada), se deberá fijar y establecer el alcance (salida) de la investigación para que se lleve a cabo de forma efectiva y adecuada. Para llegar a ello es importante tener claro cuál es el **objetivo** previsto.

Objetivo previsto:

- Si se va a requerir, por ejemplo, que el equipo simplemente descubra los hechos relacionados con un incidente concreto.
- O si se va a requerir que se tome una determinación sobre la existencia o no de un incumplimiento de una política o una posible infracción legal.

¿Qué pasaría si, como parte del proceso investigador, se enteraran de que existen infracciones adicionales, ya sean contra políticas internas, legales o incluso delictivas? En ese caso, el equipo deberá ajustar el alcance al nuevo escenario consecuencia de la labor investigadora y documentar el nuevo alcance del proceso⁹.

Es importante prever este posible escenario para adaptar el alcance inicialmente descrito y documentado de la investigación, y ajustarlo a posteriori ante la aparición de evidencias que así lo sustenten.

En todo caso, para fijar el alcance, el equipo investigador deberá tener en cuenta una serie de elementos críticos, que podríamos llamar SIGUP por sus iniciales, como son:

- Sustancia, referido a las alegaciones específicas.
- Intervalo, referido al período de tiempo a cubrir.
- Geografía, referido a las regiones y/o países afectados.
- Ubicación, referido al lugar donde presuntamente se produjo el inci-

dente.

- Personas, referido a los individuos que presuntamente cometieron la infracción.

Estos elementos críticos permitirán acotar el alcance del proceso de la investigación, facilitando la toma de decisiones a posteriori sobre el tiempo que podrá ocupar este encargo, el tamaño del equipo, los recursos, así como la composición y competencias requeridos para poder llevarlo a cabo.

Definido el alcance, toca la fase de planificación del proceso investigador, por tanto, es el momento de elaborar un plan para acometer la tarea encargada. ¿Qué elementos, mínimos, deberá contener y fijar este plan?

- Antecedentes, alcance, cronograma, propósito y objetivo de la investigación.
- Identificar quiénes deberán ser entrevistados o deben proporcionar información.
- Enumerar los recursos internos y externos necesarios. Pensemos en situaciones donde debamos acudir a expertos contables, abogados, detectives o a peritos forenses, por poner algún ejemplo.
 - Es importante, en estos casos, fijar y establecer algún tipo de tabla o matriz al estilo RACI en la que con carácter previo y en función del nivel de especialización, se determine qué perfiles deben ser requeridos y cuál será su marco de competencias asignado en función del marco legal que regule su actividad profesional. Pensemos en las competencias que la legislación de Seguridad Privada¹¹ fija en España, por ejemplo.
- Valorar medidas cautelares de índole laboral, por ejemplo, la suspensión de empleo o de acceso a determinados recursos o sistemas.

- Valorar cuáles podrían ser las posibles fuentes de pruebas y, una vez identificadas, establecer cómo abordar la preservación, recopilación y revisión de las mismas.

- Se debe contar con un procedimiento documentado que garantice la cadena de custodia.

La STS 208/2014, de 10 de marzo¹², define la cadena de custodia de la siguiente forma: *"Se viene entendiendo por la doctrina como cadena de custodia, el conjunto de actos que tienen por objeto la recogida, el traslado y la conservación de los indicios o vestigios obtenidos en el curso de una investigación criminal, actos que deben cumplimentar una serie de requisitos con el fin de asegurar la autenticidad, inalterabilidad e indemnidad de las fuentes de prueba"*.

- Dos elementos caracterizan claramente a la cadena de custodia aquí:

1. Es un sistema formal garantista
2. Garantizar que las evidencias y los resultados del dictamen objeto de pericia son coincidentes con los que se obtuvieron en la fase de recogida.

- La cadena de custodia debe cubrir cinco etapas:

1. Recogida de la evidencia.
2. Preservación y embalaje.
3. Transporte.
4. Traspaso (entrega a terceros en la investigación, por ejemplo, a peritos o abogados externos).
5. Custodia y preservación hasta el cierre del proceso investigador o juicio.

- La cadena de custodia, a su vez, se sustenta en cuatro principios básicos:

Legalidad.
Autenticidad.

Control.
Preservación.

- Y, a su vez, la cadena de custodia debe cumplir con los principios probatorios:

- Principio de aseguramiento de la prueba

- Principio de licitud de la prueba.

- Principio de veracidad de la prueba.

- Principio de necesidad de la prueba.

- Principio de obtención de la prueba.

- Principio de intermediación, publicidad y contradicción de la prueba.

- Cómo se realizarán las entrevistas, lo que incluye el calendario y las notificaciones a quiénes vayan a ser objeto de las mismas.

- Con el fin de no improvisar, será conveniente contar con un procedimiento documentado que establezca el plan de comunicación de las notificaciones a fin de no improvisar y seguir, de esta forma, los criterios fijados estándares de la organización. Es importante que este procedimiento tenga presente el diseño de diferentes estrategias de comunicación, por si resultara infructuosa alguna de ellas.

- Prever la necesidad o la posibilidad de que quién vaya a ser entrevistado solicite asistencia letrada o apoyo interno o sindical.

- En función del ámbito de actuación de la investigación y a fin de respetar la legalidad vigente, es vital identificar escenarios en que esa situación va a ser requerida y actuar en consonancia con el estatus del caso.

- Valorar si existiese alguna cuestión jurídica implicada en la investigación.

- Identificar los riesgos y/o desafíos asociados al proceso de investi-

gación y, en función de los mimos (riesgo inherente), establecer una estrategia y un plan de acción para mitigarlo y reducirlo (riesgo residual).

- Para la fase de registro, se deberá definir cómo se efectuará y llevará a cabo el registro de la investigación; a qué partes interesadas se deberá informar y, en este caso, cuándo y con qué nivel de detalle.

- Y, por último, se deberá planificar si la organización estuviera obligada a comunicar a las autoridades la presunta infracción o el resultado de la investigación.

Como hemos visto en la fase de planificación, son múltiples las aristas y las tareas a realizar para para cubrirla de forma plena y satisfactoria. En todo caso, el plan de investigación documentado va a resultar ser un documento vivo que puede sufrir modificaciones durante el propio proceso investigador. Por lo que, como es evidente, se deberá contar y aplicar los procesos de control de cambio de versión, tal como exigen las buenas prácticas de gestión.

Una vez establecido el plan de investigación se debe garantizar cuatro aspectos importantes durante todo el ciclo de vida de la investigación:

- Cómo garantizar la confidencialidad. (8.5)
- La redacción de un aviso legal escrito sobre el alcance de la confidencialidad. (8.6)
- La comunicación del aviso legal oral cuando y cómo corresponda, lo que nuevamente nos lleva a la necesidad de prever qué mensaje/s deben contemplarse en estos escenarios. (8.7)
- Evitar o parar las posibles interferencias en el proceso investigador, independientemente del origen, interno o externo. En caso de producirse, se debe registrar y escalar a la línea jerárquica establecida. (8.8).

La fase de gestión de evidencias conlleva (8.8):

EVIDENCIAS

- Recopilación y revisión de documentos (entorno analógico)

⁹ ISO 37001. CLÁUSULA 3.29

¹⁰ ISO 37008 8.3.2

¹¹ Ley 23/1992, de 30 de julio, de Seguridad Privada así como el RD 2364/1994 y la Orden del Ministerio de Justicia e Interior de 7 de julio de 1995.

¹² <https://vlex.es/vid/delito-cadena-custodia-ruptura-502207666>

¹³ NORMA UNE 71.505-2:2013 Tecnologías de la Información. Sistema de Gestión de Evidencias Electrónicas (SGEE)- Parte 2: Buenas prácticas en la gestión de evidencias electrónicas

- Obtener, asegurar, organizar y revisar de forma segura los documentos.
 - Examinar todas las pruebas aplicables.
 - Detectar documentos críticos esenciales.
 - En el caso de realizar una revisión a gran escala, valorar el uso de herramientas tecnológicas o de especialistas externos.
 - Recopilación, conservación, análisis y revisión de datos electrónicos (entorno digital)
 - Cooperación entre los equipos de investigación y el tecnológico (interno o externo).
 - Valorar el uso de plataformas tecnológicas y herramientas de búsqueda/descubrimiento. (Deben estar valoradas y aprobadas previamente)
 - Valorar el uso de tecnología y de expertos en la recuperación y revisión de datos electrónicos, garantizando la preservación electrónica de la prueba.
 - Implementar medidas adecuadas para preservar los datos y la evidencia electrónica.
- Importante aquí el apoyo del estándar UNE 71505-2: 2013¹⁴ sobre buenas prácticas en la gestión de evidencias electrónicas.
- Gestión de la identidad digital desde la triple perspectiva: Autenticación, Autorización y Auditoría.
 - Trazabilidad del proceso ejecutado y el no repudio de la misma.
 - Almacenamiento y custodia segura y con cobertura legal.
 - Definición específica de responsabilidades y el aseguramiento de la segregación de funciones de los in-

tervinientes.

- Y desde el punto de vista de la evidencia electrónica, el estándar UNE 71505-3: 2013¹⁴ enumeran algunos elementos que deben caracterizar la misma, como son:
 - Firma electrónica.
- 1. Fecha fiable de la firma.
- 2. Robustez del algoritmo a largo plazo.
- Sello de tiempo.
- 1. Garantizando el no repudio.
- 2. Relacionando las distintas evidencias para disminuir las opciones de fraude.
- Criptografía simétrica.
- 1. Para garantizar la confidencialidad.
- 1.1 Los algoritmos deben ser estándares y estar en vigor.
- 1.2 El Anexo A de UNE 71.505-3 proporciona una tabla al respecto.
- Conservación a largo plazo.
- 1. Contar con un procedimiento que garantice la conservación:
 - 1.1 Desde el punto de vista de la obsolescencia tecnológica.
 - 1.2 Proporcione confiabilidad en los procesos de renovación de claves.
- El equipo técnico involucrado deber contar con competencias tal como describe ISO/IEC 27037:2012¹⁵ en la cláusula 6.4 que señala que:
 - Deben tener competencias técnicas y jurídicas pertinentes y deben poder demostrar que están debidamente capacitados y tienen conocimientos técnicos y jurídicos suficientes para manejar adecuadamente la

posible evidencia digital. En especial:

- Deben estar adecuadamente capacitados para el manejo de dispositivos digitales en el contexto de actividades de investigación.
- Deben demostrar y mantener habilidades y competencias ante las autoridades apropiadas relevantes para el manejo de posibles evidencias digitales.
- Es responsabilidad del individuo y del empleador garantizar que están capacitados adecuadamente y que mantienen las habilidades y competencias para ello.

ENTREVISTAS

Llegado el momento de la realización de las actividades de entrevistas (8.9), el plan de entrevistas debe contemplar una estructura metodológica adecuada que consistirá en la realización de un conjunto de acciones concadenadas y estructuradas, que son:

- 1.- Preparativos.
- 2.- La realización de la entrevista en sí misma.
- 3.- El mantenimiento de los registros de la entrevista.

¿Qué acciones abarcaría el punto 1 de Preparativos?

- Diseño del plan de entrevistas.
 - Tener en cuenta el ciclo de vida de las entrevistas:
 - Inicio.
 - Apertura.
 - Cima.
 - Cierre.
- Técnicas de entrevistas.
 - Tipos de entrevistas
 - Libres; Dirigidas; de exploración; de comprobación; de información; informales.
 - Tipos de preguntas
 - Abiertas; cerradas; de sondeo; de cierre; mixtas, etc...
- Composición del equipo entrevi-

tador.

- Revisión y compilación de los documentos adecuados y pertinentes para su uso.
- Garantizar que estas se efectúen en un entorno libre de interferencias, garantizando la confidencialidad de la misma.

Durante la realización de la misma, según el punto 2 de este apartado, sería adecuado:

- Especial cuidado para contar con testigos cuando sea pertinente.
 - Quizás se precise que estén dos o más entrevistadores.
 - Grabar la sesión cuando sea pertinente y esté permitido.
 - Evitar dar la sensación de opresión al entrevistado.
- Especial atención a cuestiones como el idioma. Todos nos expresamos mejor en nuestra lengua materna, lo que podría llevar aparejado la necesidad de contar con un intérprete cualificado.
- Ante cualquier incoherencia en la declaración, será importante aclararla.
- Y en la fase de cierre, confirmar con el entrevistado los puntos abordados, garantizando de esta forma que la declaración es verdadera, precisa y exacta según el leal saber y entender; en caso de duda, se puede agregar o aclarar cualquier información contenida en la misma.
- Y, además, se deberá proceder al acta y firma correspondiente para que quede como evidencia documentada del trabajo investigador.

A fin de que el proceso de entrevista resulte de utilidad, tanto cuantitativamente como cualitativamente, el equipo entrevistador deberá:

- Prestar atención a las interacciones del entrevistado (importante el lenguaje corporal y gestual).
- Ser muy profesional y respetuoso, aunque la situación de pueda complicar.
- Escuchar más que hablar. Aquí es muy útil la regla de Pareto 80/20,

escuchar más que hablar. No nos interesa hablar, sino escuchar lo que nos tienen que contar.

- Guiar la entrevista proporcionando información precisa y correcta.

Y, para cerrar este ciclo sobre las entrevistas, queda pendiente la tercera fase, es decir el registro y mantenimiento de las entrevistas ¿Cómo enfrentarnos a este requisito del estándar?

- Documentándola y custodiándola de forma segura y confidencial.
- Comunicando por escrito la misma al entrevistado.
- Preservar los registros y documentos acordes a la política de

retención y conservación previamente establecida.

Hay, al menos, tres observaciones, que conllevan riegos, que deben tener presente los equipos de entrevistadores en esta fase:

- Las notas tomadas se deben proteger como producto de trabajo privilegiado y, si se actúa bajo dirección letrada, preservar la relación cliente/letrado.
- Las notas tomadas no deben ser compartidas con el entrevistado ni con su representante legal.
- Si la legislación nos lo permite, se podrían grabar las entrevistas, ya sea en formato video y/o audio.



¹⁴ NORMA UNE 71.505-3:2013 Tecnologías de la Información. Sistema de Gestión de Evidencias Electrónicas (SGEE)- Parte 3: Formatos y mecanismos técnicos.

¹⁵ ISO/IEC 27037:2012 Information technology- Security techniques- Guidelines for identification, collection, acquisition, and preservation of digital evidence.

¿CUÁNDO SE PODRÁ DAR POR FINALIZADO EL PROCESO DE ENCARGO DE INVESTIGACIÓN POR PARTE DEL EQUIPO INVESTIGADOR? (8.10)

Para que esto sea así deberá cumplirse el objetivo de la misma, es decir:

- Que se esté en condición de formular las conclusiones apoyadas en evidencias suficientes para el Órgano de dirección.
- Que se pueda rendir cuentas de forma plena de la encomienda.
- Que el resultado permita el despliegue de acciones correctivas y reparadoras.
- Cumplidos estos elementos o requisitos, se podrá proceder al cierre el informe de investigación encargado.

EL INFORME DE INVESTIGACIÓN (8.11)

Y cerrando este ciclo se tendrá que concluir con el preceptivo informe que recogerá los resultados encontrados y documentados como consecuencia del encargo de investigación. ¿Qué deberá recoger el informe final?

- El registro del informe.
- Ante la aparición en el horizonte

de un posible litigio, previo análisis con el área legal, evaluar la necesidad de comunicar los hechos a los reguladores o autoridades.

- Comunicar el informe de forma objetiva y precisa, según el plan de comunicación establecido.
- Recopilar, enumerar y registrar los documentos y evidencias que den respaldo suficiente al caso, de acuerdo con la evidencia documental, sonora, visual y oral.
- Dar explicación suficiente de los hechos relevantes, así como de las limitaciones y restricciones encontradas y limitantes de su trabajo.
- Evidenciar el conocimiento de la legislación afectada y aplicar la política de retención correspondiente de la organización.
- Y, por último, pero no menos importante, garantizar la seguridad de los datos para que solo se posible su uso para los fines previstos.

POSIBLES ACCIONES CORRECTIVAS O MEJORAS (9)

Comentábamos anteriormente que la investigación llegaría a su conclusión cuando, entre sus elementos, se pudiera estar en la condición de establecer

medidas correctoras o mejoras en la organización.

Pues bien, como esa cuestión forma parte de los propios objetivos del informe de investigación, el equipo deberá proponer las medidas mitigantes del riesgo evidenciado con el fin, no solo de corregir la desviación funcional y operativa, sino también con el objetivo de aportar mejoras a la gestión interna. No olvidemos que el objetivo común de los sistemas de gestión es la mejora continua y que el ciclo ACT, dentro del ciclo PDCA característicos de los estándares ISO, concluye con la atención correspondientes a las no conformidades encontradas y, seguidamente, la mejora continua.

Dentro de las medidas correctivas para enfrentarnos a esas no conformidades o incumplimientos podemos establecerlas en dos líneas de actuación, teniendo en cuenta el momento en el que se realicen:

- Por un lado, las medidas correctivas provisionales (9.2)
- Y, por otro lado, las medidas correctivas posteriores a la finalización (9.3)

Desde el punto de vista de las características comunes que deberán satisfacer las medidas correctivas o mejoras, estas deberán ser proporcionales (9.4), es decir, deberán establecerse de acu-

VENTAJA	RIESGO
Puede que sea obligatorio.	Puede dar lugar a una investigación legal más extensa y exigente.
La participación y cooperación activa, puede llevar, de forma posterior, a acciones y/o acuerdos.	Las partes interesadas toman la delantera e inician acciones legales que no tenemos previstas.
Es disuasiva ante hechos futuribles.	Puede verse incrementado el riesgo de renuncia a los privilegios que asisten en la actividad investigadora interna.
Nos permite controlar y gestionar el impacto.	Damos ventajas a la competencia o puede dar lugar a la ruptura de relaciones o acuerdos, o dar lugar a la ruptura de negociaciones ya iniciadas.

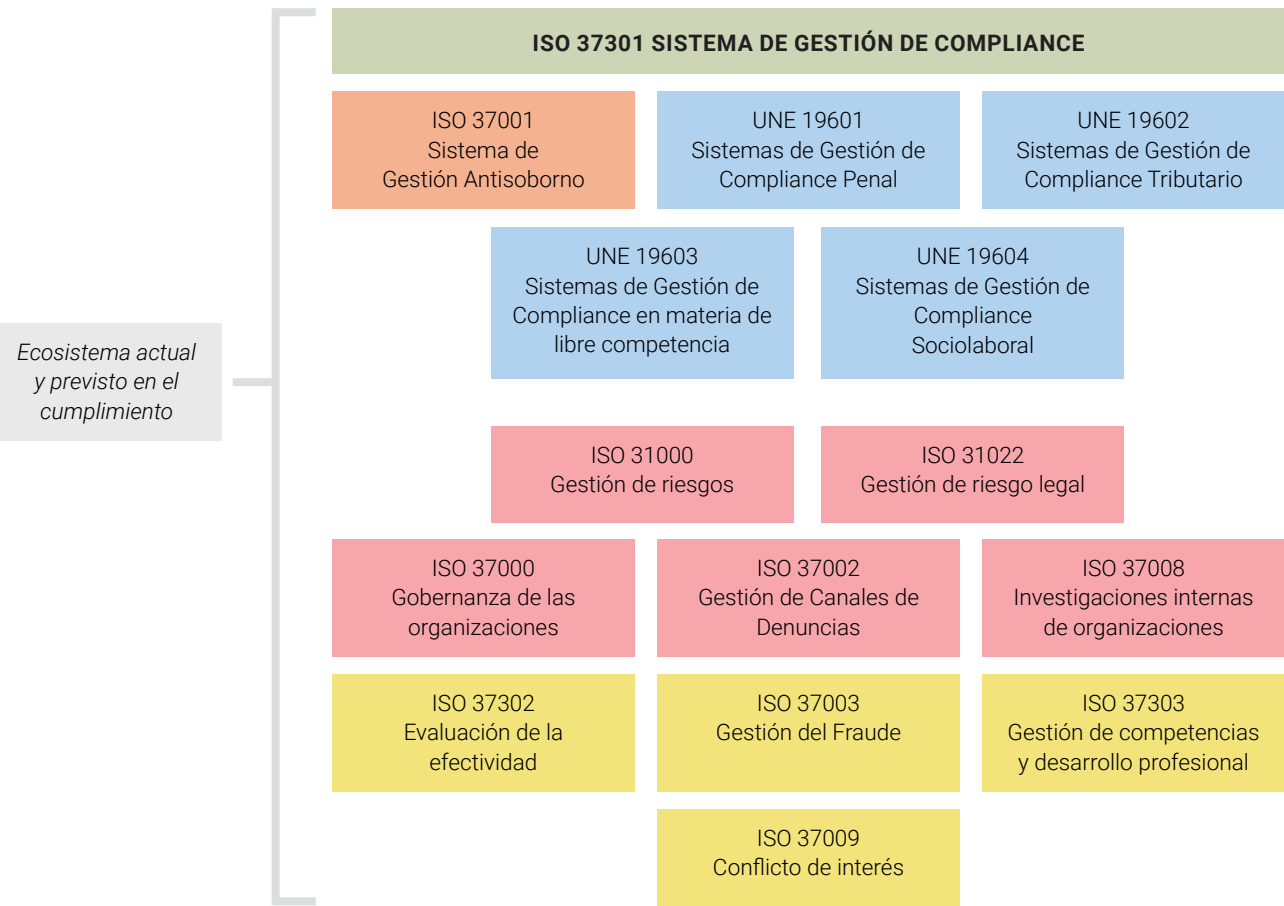
erdo con la política y/o procedimiento aprobado teniendo en cuenta la gravedad de los hechos o brechas encontrados. Y, además, se deberá ponderar si la misma se ajusta o no al programa de cumplimiento organizativo aprobado.

Ahora bien, siempre que se trata el ries-

go inherente o el gap encontrado, al implementar un control mitigante, no podemos olvidar que la acción conllevará necesariamente la modificación del comportamiento del riesgo encontrado. ¿Cómo garantizar que la modificación prevista sea la deseada? Todo plan de acción conlleva, necesariamente el mo-

nitoreo (9.5) y supervisión de las medidas implementadas con el fin de garantizar que el control se comparta tal y como hemos previsto, no se produce desviación y es eficaz y eficiente.

En especial, los riesgos tratados como consecuencia de las actuaciones de



investigación deberán ser objeto de seguimiento y atención especial durante el programa de revisión de riesgos de cumplimiento de la organización, al tratarse de riesgos que ya se han materializado, con independencia de la magnitud del impacto.

LA INTERACCIÓN CON LAS PARTES INTERESADAS (10)

Veíamos con anterioridad que la organización, solo debía tener identificadas a las partes interesadas, sino que, además, debe contar con un plan de comunicación, especialmente, en relación con la comunicación con estas partes interesadas, lo que necesariamente pasa por tener planificado la finalidad, modelo de mensajes y guiones sobre qué comunicar y cómo (10.2).

Para que la comunicación sea eficaz es importante nunca perder de vista la finalidad, que no es otra, sino la búsqueda de aportes al proceso investigador.

Para lograr esto, será importante que se aborden los temas verdaderamente importantes y se reduzca o minimice cualquier impacto negativo en la operativa organizacional (10.4). La calidad y cantidad de la información a comuni-

car debe estar previamente establecida por la organización dentro de lo que podríamos denominar su apetito del riesgo.

Se deberá contemplar cómo y cuándo se deberá comunicarse con las autoridades gubernamentales y/o los reguladores. Así como evaluar, sobre evidencia o información suficiente y necesaria, la opción de realizar una autodivulgación. En este último caso, el de la autodivulgación, será pertinente que las áreas legales y de cumplimiento validen este paso y, si fuese preciso, se recurriera a asesoramiento jurídico externo especializado.

Algo que podría ser de gran valor en los escenarios que se estén barajando la opción de la autodivulgación es contemplar los beneficios de hacerla versus los riesgos. A modo de ejemplo, se aporta una pequeña tabla que puede arrojar algo de luz en este contexto de caso de uso.

ACCIONES DISCIPLINARIAS (11)

El informe final puede aportar base suficiente y así lo deberán indicar el equipo investigador en su informe, como parte de las medidas correctivas y, en apli-

cación del régimen sancionador interno y del régimen legal que regule la relación, de las preceptivas medidas disciplinarias contra las personas infractoras y/o contra las organizaciones afectadas.

CONCLUSIÓN

A modo de conclusión, no podemos dejar de sentirnos agradecidos de contar con un nuevo estándar que viene a ir completando el puzle de normas que vienen en ayuda de las organizaciones para gobernar y gestionar sus obligaciones de cumplimiento, tanto a nivel nacional con las normas UNE¹⁶, como a nivel internacional con la familia de normas ISO¹⁷.

Por tanto, a partir de este momento, diseñar un programa de investigación e implementarlo basándonos en este nuevo estándar ISO 37008 puede ayudarnos a hacer frente a este desafío cumplimiento de una forma cabal y eficaz las regulaciones nacionales y sectoriales aplicables de un modo estandarizado y repetible.

¹⁶ UNE. Una Norma Española. Perteneciente a la Asociación Española de Normalización.
¹⁷ ISO. International Organization for Standardization

FULL&FAST, EXPERTOS EN TRANSICIÓN ENERGÉTICA. CONSTRUYENDO LA EMPRESA DE SERVICIOS DEL FUTURO

#CHARGINGTHEFUTURENOW

full&fast es una startup de base tecnológica fundada en Madrid en el 2017, especializada en la integración, financiación y comercialización de sistemas de acumulación de energía (sustitutivos de los grupos electrógenos/generadores diésel) y cargadores para vehículos eléctricos, para empresas relacionadas con los servicios y la movilidad eléctrica que no disponen de acceso a la red eléctrica, bien por estar en un lugar remoto, porque su fuente normal de suministro ha fallado, porque el suministro de potencia es limitado o porque por razones de espacio/seguridad no pueden recurrir a un generador autónomo alimentado por **combustibles** tipo diésel o gasolina.

La startup, ha desarrollado su propia tecnología de acumulación, cofinanciada por el ministerio de industria, junto con un SaaS para optimizar el consumo de energía y reducir la factura eléctrica de sus clientes (hasta un 70%). Una tecnología paralelizable, 80 veces más potente en el mismo peso y tamaño que las soluciones actuales existentes en el mercado que se integra en equipos, que funcionan de forma independiente o conectados a una infraestructura eléctrica de bajo voltaje existente para suministrar carga rápida a los vehículos eléctricos y energía a equipos eléctricos, cuando y donde sea necesario. No solo se pueden utilizar en la mayoría de los lugares sin necesidad de actualizar la red, sino que también se puede moverse fácilmente entre sitios y conectarse a paneles solares en áreas remotas.



Siendo sus clientes naturales: las flotas de vehículos eléctricos (soluciones tanto para recarga fija como recarga móvil), las empresas organizadoras y proveedoras de eventos, las empresas distribuidoras y comercializadoras de energía eléctrica, las empresas de la construcción y empresas de producciones cinematográficas (full&fast).

La primera idea de negocio surgió cuando fuimos conscientes de la necesidad de flexibilizar el acceso a la recarga, a las empresas de flotas de uso intensivo de vehículos eléctricos que estaban de-

sembarcando en Madrid. Empresas de carsharing como Car2Go o Zity, que requerían de un equipo de 500 personas de media por cada 1.000 coches, solo para gestionar la recarga del vehículo eléctrico, es decir mover los coches aparcados en los distintos puntos de la ciudad a sus bases para recargarse, para luego volver a ponerlos en la calle, a disposición de los usuarios.

De la necesidad de evitar tener que recurrir a ubicaciones fijas para la recarga, la startup fue reforzando su propuesta, con la adición de otros servicios y sec-



tores que también requerían de flexibilidad, en el acceso a una energía limpia o verde.

Hoy por hoy, son los grupos electrógenos/generadores diésel, los que suplen la falta de acceso a la energía y estos funcionan quemando combustible para producir electricidad, con sus consabidas emisiones y restricciones regulatorias.

Una de las grandes limitaciones en el acceso a la energía "verde" es, la dificultad para lograr ponerla a disposición de quien la necesita, justo en el momento y en el lugar donde la necesita y sin incurrir en costes elevados.

Básicamente, a diferencia de otras, la energía eléctrica depende de la existencia de una red para su distribución y a su vez, el acceso a esta energía viene condicionado por generación sostenible existente (no siempre hace sol y no siempre sopla el viento) para poder suministrarla en la potencia y capacidad necesaria.

¿Y si pudiéramos disponer de más energía, en el momento que queramos, sin necesidad de ampliar la potencia contratada?, ¿Y si pudiéramos incluso tener más potencia que la que puede aportar nuestra instalación? ¿Y si fuera posible disponer de un equipo que almacene y entregue energía? ¿Es la energía eléctrica capaz de llegar incluso a donde no llega la red de distribución?

Para full&fast, la respuesta a todas esas cuestiones es sí, en todos los casos. Para nosotros, la necesidad de flexibilizar el acceso a la energía eléctrica mediante lo que conocemos como generación (potencia) distribuida, apoyada en sistemas de acumulación eficientes y portátiles, es nuestro objetivo estratégico como empresa. Necesidad que hemos desarrollado bajo un servicio de pago por uso, que hemos bautizado, como "Green Eel", ("Anguila verde") inspi-

rado en la imagen de una anguila eléctrica y la energía limpia.

<https://www.fullandfast.com.es/servicio-alquiler-equipos-de-energia-portables.php>

GreenEel, es un servicio financiero de pago por uso (ya sea en la modalidad de renting o leasing) vinculado a sistemas de acumulación y/o cargadores de vehículo eléctrico, bajo dos premisas:

- Portabilidad. Despliegue de infraestructura en un 1 solo día
- Flexibilidad. Adaptados a las necesidades cambiantes de los negocios de nuestros clientes y demandas estacionales de energía.

Junto con ese objetivo nuestra visión de negocio es llegar a convertir a full&fast en una herramienta para alcanzar los objetivos de sostenibilidad para nuestro futuro. Garantizando el acceso a una energía asequible, segura, sostenible y moderna para todos. Construyendo Infraestructuras resilientes, promoviendo la industrialización inclusiva y sostenible y fomentando la innovación. Logrando que las ciudades y los asentamientos humanos sean inclusivos, seguros, resilientes y sostenibles (ODS 7,9 y 11).

Si una actividad económica debe generar beneficios atendiendo a la agenda 2030, ¿se puede realmente atender las necesidades de los más pobres de un país en desarrollo, incluso con un enfoque centrado en la base de la pirámide económica? ¿cómo demostramos el valor adicional generado por las empre-



PROYECTOS INTEGRALES A LA MEDIDA DE CADA CLIENTE



DONDE QUIERA QUE ESTE, EL TIEMPO QUE LO NECESITE



TODOS LOS CARGADORES Y EMPLAZAMIENTOS BAJO UN MISMO SISTEMA DE GESTIÓN



MÁS POTENCIA PARA UNA CARGA MÁS RÁPIDA SIN COSTES HUNDIDOS



AHORRO DEL 20% EN COSTOS DE INSTALACIÓN Y DEL 70% EN EL COSTOS OPERATIVOS

sas? En full&fast demostramos tanto un ahorro del 100% en las emisiones contaminantes generadas por un grupo electrógeno, como rentabilidad, midiendo las toneladas de CO2 reducidas, los litros de combustible ahorrados y los kW de energía instalados.

Esto último, un claro desafío, dada la información asimétrica en torno a las prácticas empresariales, subrayando y apelando a la Responsabilidad Social Corporativa (RSC), la importancia y seguimiento de la cuestión relativa a cómo promover un mejor comportamiento del sector privado, en línea con los objetivos ODS.

¿NUESTROS VALORES?

La sostenibilidad y el compromiso con el cuidado del medio ambiente

En full&fast estamos alineados con la agenda 2030 para un desarrollo sosteni-

ble, con un empeño especial por garantizar el acceso a una energía verde en nuestros servicios. El 100% de nuestros equipos emiten cero emisiones. El compromiso medioambiental, así como la innovación, conforman los ejes de nuestro desarrollo y por ello priorizamos el uso de energía de origen renovable en nuestros proyectos.

La eficiencia y la innovación

Entendemos la innovación como un proceso continuo de generación de valor añadido. Innovación en todos los procesos que permiten ofrecer una mejor solución a nuestros clientes. Innovación en nuestro modelo de negocio. Innovación en nuestra tecnología.

La responsabilidad

full&fast cree en un futuro en el que la correcta gestión de la energía limpia, permitirá que las nuevas generaciones

disfruten de un planeta más sostenible.

La transparencia

Los procesos en nuestra empresa, se rigen por criterios de transparencia, tanto en la gestión de personal y económica, como en los criterios de elección de proveedores y socios. En full&fast tenemos en cuenta la aportación de nuestros socios, ahora y en el futuro, para garantizarnos a nosotros y a nuestros clientes, la mejor elección y la más transparente.

¿Y QUÉ VIENE DESPUÉS DE LA AGENDA DEL 2030? ESPAÑA 2050

Priorizar la educación, neutralidad climática (cero emisiones netas) con una generación sin combustibles fósiles, frenar la despoblación de los pueblos, cambios en el IRPF... son algunas de las medidas que recoge el plan de España 2050 y que busca alinearse con el acuerdo el Acuerdo de París. Acuerdo

que habla de la visión de llevar a cabo plenamente el desarrollo y la transferencia para mejorar la resiliencia al cambio climático y reducir las emisiones de gases de efecto invernadero.

Por nuestra parte, seguiremos trabajando en facilitar el acceso a la energía y recarga de vehículo eléctrico, sin ruidos, sin emisiones y sin olores, a todas las empresas y servicios, que necesiten de flexibilidad en su camino a la electrificación y la neutralidad en emisiones. Evitando la conocida como fiscalidad ambiental de los ODS directamente relacionados con medidas de protección ambiental.



"MÁS DE 40 CLIENTES Y PRESENCIA EN TODA EUROPA. IMPLEMENTAMOS SOLUCIONES DE ENERGÍA Y DE RECARGA DE VEHÍCULOS ELÉCTRICOS ESCALABLES Y FLEXIBLES"



"ACCESO A LA ENERGÍA QUE NECESITAS CUANDO LA NECESITAS"



W3 CANAL DE DENUNCIAS
Minimiza los riesgos de tu empresa



REPERTORIO JURISPRUDENCIA

Por Manuel Montesdeoca de la Fuente

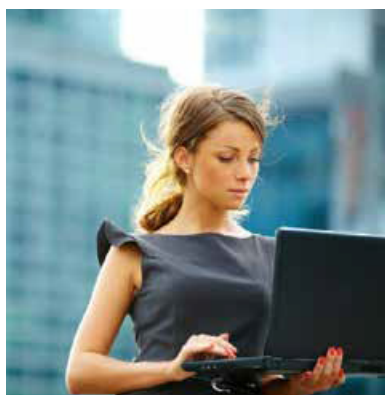
W3 COMPLIANCE

"W3 canal de denuncias, el canal interno de información que cumple todos los requerimientos de la ley 2/2023 reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción"



La aplicación es muy intuitiva y admite denuncias tanto anónimas como denuncias confidenciales, todas ellas asociadas a las empresas que se hayan dado de alta en el sistema.

En el caso de denuncias confidenciales, el denunciante recibe correos que le van avisando e informando sobre los cambios de estado de su denuncia.



El programa también permite plantear consultas, lo que es una consecuencia de nuestro empeño por reforzar el aspecto preventivo de las conductas que pueden generar un riesgo para la organización.

La aplicación cuenta con los más **altos estándares de seguridad:**

Comunicación cifrada (https) con la aplicación

Base de datos cifrada en el servidor

Copias de seguridad con cifrado adicional

Supresión de datos a los tres meses del registro de la denuncia

Servidor de aplicaciones y datos en España certificado en el Esquema Nacional de Seguridad



Se ofrecen versiones que se pueden consultar en la web:

<https://www.w3compliance.com>

Todas las versiones incluyen:

Soporte Técnico permanente

Propuesta de calificación jurídica de los hechos

Informe de recomendaciones y resultados



SENTENCIA DEL TRIBUNAL SUPREMO 330/2023, DE 10 DE MAYO DE 2023, REC. 3629/2021

Ponente:
Magro Servet, Vicente.

La sentencia es de interés por cuanto aun no refiriéndose a una condena de persona jurídica analiza la responsabilidad de control del Compliance office que no se puede extender a otros ámbitos diferentes del de la responsabilidad penal de las personas jurídicas regulada en el art. 3 bis del C.P.

La sentencia resuelve los recursos de casación de tres personas jurídicas que habían sido condenadas por la Audiencia Provincial de Valladolid, por diversos delitos relacionados con su pertenencia o vinculación con una asociación sin ánimo de lucro. En concreto, el presidente de la asociación, que habría cometido los delitos aprovechándose del cargo que ostentaba en la misma, había sido condenado por administración desleal continuada y falsedad en documento oficial efectuada por particular en concurso medial con un delito continuado de estafa agravada, apropiación indebida agravada y falsedad continuada en documento mercantil. Su mujer había sido condenada por delito continuado de falsedad en documento oficial efectuada por particular en concurso medial con un delito continuado de estafa agravada. Finalmente, un tercer condenado, que también ocupaba un cargo directivo en la asociación, había sido condenado por delito continuado de apropiación indebida.

La sentencia, después de analizar de forma pormenorizada las pruebas valoradas por la sentencia recurrida, confirma las condenas de dos de las personas físicas, el presidente y el vicepresidente de la entidad, absolviendo, por el contrario a la mujer del primero, al no concurrir en ella e el elemento subjetivo de lo injusto del delito de falsedad en documento oficial en concurso con estafa. Su supuesta participación en la comisión de dichos delitos se limita al envío de documentos oficiales a la Administración, en el marco del contrato profesional que le une a la asociación, sin que por ello pueda presumirse que conociera la falsedad del contrato en que se basaba el envío de dichos documentos.

Manifiesta el Tribunal Supremo que se le condena, en realidad, simplemente por presumir que, siendo la mujer del presidente de la asociación y siendo, además, economista profesional, debía

inexorablemente conocer el proceso operativo delictivo. Dicha conclusión es rechazada por el Tribunal que establece expresamente en su F.J 7º que, además, los hechos probados **no recogen el conocimiento de la recurrente como tramitadora de lo que se le había encargado, sin que sus conocimientos profesionales den lugar, por sí mismos, a una actividad delictiva por tener que conocer el delito cometido por un tercero, a modo de un compliance officer que tuviera obligaciones de prevenir, o evitar, los delitos cometidos por otra persona, aunque éste fuera su marido, o poner medidas de control preventivo a modo de cumplimiento normativo para evitar un delito, cuando no hay razones objetivas para asegurar el dolo de la recurrente de que se hubiera falsificado el contrato inicialmente, y que sus trámites posteriores fueran para coadyuvar en la ejecución del previo delito cometido por su marido.**

Igualmente indica el Tribunal Supremo, para fundamentar la absolución de la condenada, que *en la sentencia se plasma una especie de actuación colaborativa presunta de la mujer casada con respecto a la ilícita económica del marido, no pudiendo articularse una especie de exigencia hacia la mujer casada de posicionarse en la relación matrimonial como si fuera un programa de compliance que evite la actuación ilícita de los delitos cometidos por el marido, a modo de una exigencia de conocer obligatoriamente la ilicitud económica perpetrada por aquél, ya que ello supondría una presunción contra un acusado en un proceso penal, sin exigencia de la prueba debida, sobre todo cuando se trata de un elemento subjetivo del injusto, como es el conocimiento de la ilicitud previa, que en este caso se presume cuando los hechos se remontan al año 2004, y no solamente ello, sino la colaboración de la mujer casada con el ilícito perpetrado por el marido años antes de la actuación de la recurrente, y como mujer casada actual desde el punto de vista profesional, sin que el conocimiento técnico de la misma por ser economista tenga que suponer una presunción contra ella de que por su categoría profesional deba conocer la ilicitud perpetrada por su marido años antes de la colaboración que se le solicita.*

SENTENCIA DEL TRIBUNAL SUPREMO 585/2023, DE 12 DE JULIO DE 2023, REC. 5872/2021

Ponente:
Magro Servet, Vicente.

La Sentencia resuelve los recursos de casación presentados por una persona física condenada previamente por la Audiencia Provincial de Barcelona, como autora de un delito continuado de estafa del artículo 248, 249 y 250.1.5º del C.P., en relación con el art. 742 CP, en concurso medial del art. 77 CP con un delito continuado de falsedad en documento mercantil del artículo 392.1 y 390.1.2º y 3º; así como el de una persona jurídica condenada como partícipe a título lucrativo.

Lo relevante de esta sentencia, a los efectos que nos ocupan, es la reflexión que realiza el Tribunal, en una línea jurisprudencial ya habitual, sobre la importancia de los programas internos de compliance ya que, **en casos como el enjuiciado, la falta de un adecuado control interno que evite el fraude interno en las personas jurídicas con la mecánica de un adecuado compliance que actúe como factor de corrección y prevención de estas ilicitudes, no saldrían en muchos casos a la luz si el autor no lo confesara, a menos que una correcta auditoría lo detecte, o que la aplicación del programa de compliance actúe en estos casos de forma eficaz si reúne los requisitos de implementación adecuados a los estándares exigibles, y detecte lo que se denomina ex art. 31 bis CP que se han eludido los mecanismos de control de forma fraudulenta.**

SENTENCIA DEL TRIBUNAL SUPREMO 833/2023, DE 15 DE NOVIEMBRE DE 2023, REC. 7256/2021

Ponente:
Magro Servet, Vicente.

La Sentencia resuelve el recurso de casación presentado por las representaciones procesales de una serie de personas físicas que habían sido condenadas por la Audiencia Provincial por delitos de falsedad en documento mercantil, y a alguno de los acusados, además, por blanqueo de capitales y por delitos contra la Hacienda Pública.

Los hechos juzgados se refieren a un grupo de personas físicas, que ejercen el control y la administración de hecho de determinadas sociedades, que emiten y venden facturas falsas a terceros. Se

trata de sociedades instrumentales que carecen de funcionamiento real y que han sido utilizadas de forma exclusiva para este fin defraudador. Solo alguna de las que se citan tenía funcionamiento real, pero también han operado con su estructura para el fin delictivo.

Para llevar a cabo su actividad delictiva, los acusados contaban con una amplia red de sociedades instrumentales, personal e intermediarios, y una infraestructura de medios y servicios que extendía su actuación a gran parte del territorio nacional, con la finalidad de defraudar a la Hacienda Pública.

La emisión de las facturas que no amparaban operaciones reales se realizaba, en general, por sociedades instrumentales, que carecían, en realidad, de medios materiales y humanos para llevar a cabo las actividades que se documentaban en esas facturas. No obstante, alguna de esas empresas sí que desarrollaba una mínima actividad mercantil real, contando con esa infraestructura, medios y personal necesarios, lo que dificultó el control por parte de la Hacienda Pública.

Para dar mayor verosimilitud, se simulaban también compras ficticias y las correspondientes consignaciones en los modelos tributarios. De esta manera, además, no se tributaba por las ventas ficticias, al ser neutralizados esos ingresos con otros gastos y cuotas de IVA soportado o pagado, que también eran falsas. Existían, por tanto, diversos escalones en la actuación ficticia, colocando a diversas sociedades instrumentales en cada uno de esos escalones o fases.

En los recursos de casación que analiza la sentencia **interesa destacar, a los efectos de cumplimiento normativo, las referencias que realiza la sentencia sobre la prueba pericial o testifical-pericial de los funcionarios de Hacienda Pública, que no puede quedar sin valor o contenido por su posición ad extra en la agencia tributaria y que luego comparece ad intra en el proceso penal cuando ha llevado a cabo una investigación y que, más tarde, pueden acudir al juicio oral en su condición de testigos-peritos, porque pueden ser interrogados por lo que han visto cuando intervienen in situ, y por sus conclusiones a raíz de sus conocimientos en materia tributaria.**

Continúa señalando la Sentencia que, además, el testimonio de los funcionarios de Hacienda *ha sido sometido a la debida contradicción y si las defensas*

quieren poner en duda algún extremo de su informe pueden plantear sus alegaciones en la práctica de la prueba e interrogar a los funcionarios cuando comparezcan el día del juicio. Pero no puede cuestionarse sin más la utilización por el tribunal del informe técnico expuesto en el plenario y su valoración como prueba para el dictado de la condena como delito contra la hacienda pública.

Por lo expuesto, la sentencia considera que ese testimonio no es prueba testifical, sino testifical-pericial, o pericial; **puesto que no son meros testigos que cuentan lo que ven, sino que completan lo que ven con lo que saben como expertos de la agencia tributaria en la materia sometida a enjuiciamiento.**

A continuación, la Sentencia comentada aclara que lo que no puede hacer el perito es fijar el derecho aplicable, razón por la cual, no se admiten las periciales en derecho, con la salvedad de las pruebas periciales en materia de compliance en los procesos en que se dirima la posible responsabilidad penal de las personas jurídicas. Incluso en estos casos, como aclara la sentencia, la pericial, judicial (si la insta el Fiscal), que no jurídica, consiste en la concurrencia o no en la empresa de un programa de cumplimiento normativo. Todo ello, evidentemente, a los efectos de la posible exoneración o atenuación de la pena.

Merece destacarse igualmente que algunas de las defensas incluyen como motivo de impugnación de la sentencia en sus respectivos recursos, la falta de citación expresa al acto del juicio oral de las sociedades, personas jurídicas, alegando por ello indefensión. Niega, sin embargo, el Tribunal Supremo dicha supuesta indefensión, al entender que no ha habido enjuiciamiento ni, por tanto, condena para las mismas y que, en última instancia, las sociedades son entidades puramente instrumentales, que no desarrollan una actividad mercantil real, sin ingresos, ni beneficios, con lo que sus titularidades formales son, en realidad, propiedad única y exclusiva de los acusados, personas físicas, que son quienes ostentan la dirección, gestión y control de cada una de ellas.

La sentencia alude en este punto a una cuestión que es ya recurrente en muchas sentencias relativas a condenas por delitos cuya comisión se lleva a cabo a través de sociedades aparentes, creadas con la única o casi única finalidad de generar el delito, como una simple pantalla, sin entidad real suficiente.

Por ende, estamos ante una sociedad instrumental, que si bien formalmente es una persona jurídica, materialmente carece del suficiente desarrollo organizativo para ser diferenciada de la persona física, sin que pueda por ende serle de aplicación el art. 31 bis; no sólo ya por la inviabilidad de implantación de los programas de cumplimiento normativo (vid. STS 534/2020, de 22 de octubre); sino muy especial y previamente por el desvelamiento declarado en sentencia de la forma societaria, que hace inoponible su existencia como ente diferenciado de su administrador. (STS 264/2022, de 18 de marzo).

Mas recientemente en la sentencia 108/2019, de 5 de marzo, recordábamos que "Conforme señala la sentencia de esta Sala núm. 154/2016, de 29 de febrero, "... la sociedad meramente instrumental, o "pantalla", creada exclusivamente para servir de instrumento en la comisión del delito por la persona física, ha de ser considerada al margen del régimen de responsabilidad del artículo 31 bis, por resultar insólito pretender realizar valoraciones de responsabilidad respecto de ella, dada la imposibilidad congénita de ponderar la existencia de mecanismos internos de control y, por ende, de cultura de respeto o desafección hacia la norma, respecto de quien nace exclusivamente con una finalidad delictiva que agota la propia razón de su existencia y que, por consiguiente, quizás hubiera merecido en su día directamente la disolución por la vía del artículo 129 del Código Penal , que contemplaba la aplicación de semejante "consecuencia accesoría" a aquellos entes que carecen de una verdadera personalidad jurídica en términos de licitud para desempeñarse en el tráfico jurídico o, en su caso, la mera declaración de su inexistencia como verdadera persona jurídica, con la ulterior comunicación al registro correspondiente para la anulación, o cancelación, de su asiento. (STS 534/2020, de 22 de octubre).

Ambas sentencias hacen una remisión a la Circular de la FGE 1/2011 de 1 de junio, relativa a la responsabilidad penal de las personas jurídicas conforme a la reforma del Código Penal efectuada por Ley Orgánica número 5/2010, Circular que su apartado II.1, dedicado a los "Entes colectivos dotados de personalidad jurídica", contiene las siguientes consideraciones:

No obstante lo dicho hasta este momento, en los casos en los que se detecte la existencia de sociedades pantalla o de

fachada, caracterizadas por la ausencia de verdadera actividad, organización, infraestructura propia, patrimonio etc., utilizadas como herramientas del delito o para dificultar su investigación -el ejemplo más clásico y nutrido lo encontramos en las sociedades trucha de las tramas de defraudación del IVA-, nada obsta a recurrir bien a la figura de la simulación contractual, bien a la doctrina del levantamiento del velo -que en sede penal constituye básicamente un recurso de búsqueda de la verdad material-, a los efectos de aflorar a las personas físicas amparadas por la ficción de independencia y alteridad de la sociedad pantalla. Así, aun a pesar de que desde el punto de vista estrictamente formal, una empresa pantalla puede gozar de personalidad jurídica y por tanto, ser potencial responsable de conductas delictivas conforme al art. 31 bis del Código Penal, en los aludidos supuestos de abuso de la forma social, se ajustarán más a la realidad las opciones apuntadas en la medida en que posibilitan la imputación directa de las personas físicas por los delitos cometidos tras el manto de opacidad que otorga la sociedad ficticia [...].

"Por otra parte, en aquellos otros casos en los que se produzca una identidad absoluta y sustancial entre el gestor y la persona jurídica, de modo tal que sus voluntades aparezcan en la práctica totalmente solapadas, sin que exista verdadera alteridad ni la diversidad de intereses que son propias de los entes corporativos -piénsese en los negocios unipersonales que adoptan formas societarias-, resultando además irrelevante la personalidad jurídica en la concreta figura delictiva, deberá valorarse la posibilidad de imputar tan solo a la persona física, evitando la doble incriminación de la entidad y el gestor que, a pesar de ser formalmente posible, resultaría contraria a la realidad de las cosas y podría vulnerar el principio non bis in idem".

SENTENCIA DEL TRIBUNAL SUPERIOR DE JUSTICIA DE MADRID, SALA DE LO CIVIL Y PENAL 375/2023, DE 19 DE OCTUBRE DE 2023, REC. 446/2023

Ponente:
Goyena Salgado, Francisco José.

La Sentencia resuelve el recurso de apelación presentado por la Abogacía del Estado, en representación de la Agencia Estatal de la Administración Tributaria, contra una sentencia de la sección 5ª de

la Audiencia Provincial de Madrid, que había condenado a una persona física por un delito contra la hacienda pública, y absuelto a la persona jurídica (sociedad mercantil) del que la persona física era administrador.

El recurso de apelación se dirige, por tanto, contra la absolución de la persona jurídica, respecto de la cual, no aprecia la Audiencia Provincial de Madrid la concurrencia de delito. Al recurso de apelación, además, se opone el Ministerio Fiscal que solicita su desestimación y, por tanto, la confirmación de la sentencia también en el pronunciamiento absolutorio penal a favor de la persona jurídica.

Teniendo en cuenta que los hechos por los que había sido condenado el administrador persona física consistían básicamente en dejar de pagar conscientemente la cuota tributaria del IVA correspondiente al año 2014, falseando la deducción de cuotas ficticias de IVA soportado, con el consiguiente beneficio a costa de la Hacienda Pública, la sentencia de la Audiencia Provincial entendió que no cabía atribuir responsabilidad penal a la persona jurídica, por no ser autora de los hechos, y no por considerar que la persona jurídica fuera en este caso una mera sociedad instrumental o pantalla para la comisión del delito por la persona física, admitiendo que se trata de una empresa real, que opera en el mercado y desarrolla una actividad real. No obstante, aunque sea formalmente una sociedad de responsabilidad limitada, opera como si se tratara de una sociedad unipersonal, confundiéndose la voluntad social con la voluntad de su administrador único, porque la mercantil carece de voluntad propia diferenciada de la de su administrador único.

Continúa la sentencia de la Audiencia, en defensa de la inexistencia de responsabilidad penal por parte de la persona jurídica, indicando que un indicio de que la voluntad social coincide con la del administrador es que la empresa careciera de mecanismos de "compliance" o cumplimiento normativo.

En contra de los criterios de la Abogacía del Estado, la sentencia del TSJ de Madrid confirma el criterio de la Audiencia, al entender que para imponer responsabilidad penal a la persona jurídica, se requiere que la acción de la persona física esté relacionada con fallos organizativos o de funcionamiento en la gestión, control, supervisión o vigilancia de la entidad, en la prevención del

delito en cuestión. Esta interpretación, además, es la más acorde con los principios rectores del derecho penal, como el de culpabilidad subjetiva, de acuerdo con el cual, en términos del propio TSJ, la responsabilidad penal de la persona jurídica habrá de serlo por la perpetración de su propio hecho corporativo y en función del reproche culpabilístico de dicho hecho, al margen y obviando criterios de responsabilidad objetiva, como supondría hacerla responsable por una simple transferencia acrítica del hecho cometido por la persona física; el cometido por ésta, como hecho de conexión, podría ser presupuesto de la comisión del de aquélla, pero no serviría como fundamento, que ha de buscarse en uno propio. En esta misma línea se manifiesta la STS 747/2022, de 27 de julio de 2022, cuando afirma que "el régimen de responsabilidad penal de personas jurídicas exige una mínima alteridad de la persona jurídica respecto de la persona física penalmente responsable. Cuando el condenado penalmente como persona física es titular exclusivo de la sociedad, no resulta factible imponer dos penalidades sin erosionar, no ya solo el principio del non bis in idem, sino la misma racionalidad de las cosas".

Finalmente, la sentencia comentada añade una nueva razón para confirmar la sentencia absolutoria, citando la STS 576/2018, de 21 de noviembre, que señala que la jurisprudencia europea no permite en estos casos revisar las pruebas personales por el Tribunal que no disfrutó de la intermediación de su práctica; ni tampoco revisar el juicio de culpabilidad, sin audiencia del acusado (SSTEDH de 10 de marzo de 2009, caso Igual Coll c. España; 22 de noviembre de 2011, caso Lacadena Calero c. España; 13 de diciembre de 2011, caso Valbuena Redondo c. España; 20 marzo 2012 -en concreción a la voluntad de defraudar a la Hacienda Pública-, caso Serrano Contreras c. España; 27 de noviembre de 2012, caso Vilanova Goterris c. España; 8 de octubre de 2013, caso Nieto Macero c. España; 8 de octubre de 2013, caso Román Zurdo c. España; 12 de noviembre de 2013, caso Sainz Casla c. España; 8 de marzo de 2016, caso Porcel Terriba s y otros c. España; o 29 de marzo de 2016, caso Gómez Olmeda c. España; 13 de junio de 2017, caso Atutxa c. España); audiencia que no tenido lugar, ni tampoco se encuentra prevista en la ley.

EUCompliance news

Asociación Europea de Abogados
y Economistas en Compliance

Passeig Vergaguer, 120, Entlo. 4ª
Igualada (Barcelona)
Telf.: +34 938 049 038
info@aeaecompliance.com



www.aeaecompliance.com

Colabora



Patrocina

