"Las pymes por fin ven el valor innegable del compliance"

Berta Aguinaga
Socia responsable de Penal Económico y *Compliance* de Ontier

Borja *Carrascosa*

Las empresas operan en un entorno cada vez más regulado, y la hiperconectividad global obliga a los directivos a gestionar muchos riesgos de distinta naturaleza. En este contexto, el entorno digital ha disparado el volumen de información que se conoce y se comparte -o se "roba"- de una compañía, de su actividad y de sus trabajadores. La aparición del concepto de *compliance* o cumplimiento normativo responde a una necesidad de agrupar la gestión de todos esos posibles riesgos, tanto tangibles, como intangibles. Berta Aguinaga, socia responsable de Penal Económico y *Compliance* de Ontier, analiza con Capital la evolución de este fenómeno en el ámbito corporativo.

¿Se han consolidado los departamentos de *Compliance* dentro de la estructura de las empresas?

Sí, es el momento de hablar de la consolidación del *compliance* (cumplimiento normativo), y no solo penal, en nuestro sistema jurídico-económico. Estamos en un momento de madurez. Hace ya cuatro o cinco años se está empleando mucho el concepto de *compliance* corporativo ("*corporate compliance*") para referirse al cumplimiento, por parte de las empresas, de las normas que aplican a su actividad y a la gestión de sus negocios. Tenemos, por un lado, materias sujetas a lo que podríamos llamar "hard law" o derecho vinculante (como la prevención de riesgos laborales, penales, la protección de datos o el medio ambiente) cuyo cumplimiento es obligatorio y, por otro, materias que, por el momento, no cuentan con una norma específica en materia de *compliance* que obligue a su cumplimiento (como el *compliance* fiscal) y, por tanto, sujetas a lo que podríamos llamar "soft law" o derecho indicativo, no vinculante. En todo caso, la tendencia es, sin duda, que las organizaciones integren todos los riesgos corporativos bajo un mismo sistema y metodología. Los riesgos operativos, los reputacionales, los financieros y los propios de *compliance*, entre otros, se gestionarán cada vez más bajo un mismo esquema. También se incluye aquí el gobierno corporativo, la Responsabilidad Social Corporativa (RSC) y la ética empresarial. La idea es trascender los mínimos de cumplimiento (obligatorios) para alcanzar los máximos de excelencia (voluntarios, como la RSC o las políticas ESG). El *compliance* trasciende la normativa y es necesario para trasladar a los diferentes grupos de interés (*stakeholders*) una imagen de compromiso con la cultura ética, con el buen hacer y con la transparencia.

La sostenibilidad se ha convertido prácticamente en una obligación para las empresas. ¿Qué impacto puede tener para una empresa la no implementación de políticas sostenibles?

Actualmente, no implementar políticas ESG (*Environmental, Social & Governance*) –esto es, medioambientales, sociales y de gobierno corporativo– puede tener repercusiones negativas para una com-


“ES IMPORTANTE
PRESTAR UNA PROTECCIÓN
EFECTIVA Y EQUILIBRADA
A LOS DENUNCIANTES
INTERNOS DE LAS EMPRESAS”

pañía. Es un hecho constatado que las empresas que implantan medidas y políticas orientadas a contribuir a los ODS (Objetivos de Desarrollo Sostenible) presentan un menor coste de capital, menor volatilidad y menos casos de soborno, corrupción y fraude. En este sentido, aunque es cierto que todavía hay un conocimiento más profundo de la materia en las grandes empresas, el Covid-19 ha supuesto un impulso importante en las medidas de flexibilización horaria, conciliación e igualdad también en pymes. De hecho, desde el pasado 7 de marzo de 2021 las empresas con más de 100 trabajadores están obligadas a contar con un Plan de Igualdad; obligación que a partir de marzo de 2022 se extenderá también a empresas con más de 50 trabajadores. El incumplimiento de esta obligación lleva aparejada sanciones que pueden alcanzar los 187.515 euros. Las acciones orientadas a atender los ODS, sin duda refuerzan la cultura de cumplimiento y generan muchas ventajas competitivas, pues no solo fortalecen la relación de la empresa con sus grupos de interés, sino también su reputación e imagen corporativa. Tras la pandemia, estas acciones se han visto todavía más reforzadas.

¿Cómo se percibe el *compliance* en España?

Parece que no solo las grandes empresas, sino también las pymes de nuestro país, han dejado de ver la inversión en *compliance* como un gasto desvinculado del negocio, para verlo como un elemento fundamental que le añade un valor innegable. Supone una garantía de buen hacer, de compromiso con la cultura ética y de cumplimiento y de una nueva manera de hacer negocios. Hoy, tener un modelo de *compliance* implantado, en muchos casos, es un requisito para poder entablar relaciones comerciales tanto de ámbito nacional, como internacional. Sobre todo, si se trata de grupos empresariales transnacionales o cotizadas. A esta evolución natural del *compliance* hay que unir un factor absolutamente determinante del contexto socio-económico actual como es la pandemia del Covid-19, que implica la aparición de nuevos riesgos que están siendo analizados por las empresas españolas y, sobre todo, un incremento exponencial de la probabilidad de que se materialicen determinados riesgos (ya previstos en los modelos de prevención de las empresas) inherentes a la gestión de cualquier compañía. Por tanto, identificar los potenciales riesgos penales a los que se enfrentan las empresas y sus respectivos gestores para poder prevenirlos, detectarlos en caso de que se materialicen y reaccionar frente a ellos, debería ser una prioridad en todas las organizaciones.

Tengo una pyme, ¿realmente necesito un departamento de *Compliance*?

Sí, las pymes también deben implantar mecanismos de prevención de riesgos, y, de hecho, están llamadas a ser piezas fundamentales en el desarrollo del cumplimiento normativo. Prácticamente no hay ya ningún empresario que no entienda que el *compliance* es, como decía, una fuente de valor, que genera credibilidad y confianza. Cualquier organización, con independencia de su tamaño o estructura, puede constituir por sí sola un foco delictivo, y, más todavía, si atendemos al modo en que está evolucionando el mundo actual de los negocios. Pese a lo anterior, sí es cierto que el Código Penal (en su artículo 31 bis) dedica un apartado específico (3º) a las pymes para facilitar la implantación de sus respectivos modelos de gestión de riesgos penales. Una de las principales diferencias entre el *compliance* penal de grandes empresas y pymes es que, en las segundas, las labores de *compliance* pueden ser asumidas directamente por el órgano de administración. La razón de esta regla particular es la propia naturaleza de los modelos de prevención de delitos. Y es que si una organización quiere beneficiarse de la exención de responsabilidad penal derivada de la implantación de un *compliance* eficaz, éste debe ajustarse a las peculiaridades de cada empresa, entre ellas, su tamaño. Este modelo será más simple en estructura y recursos cuanto más sencilla sea la organización. Es lo que la Fiscalía General del Estado llama “una razonable adaptación a su propia dimensión”. La base del diseño e implantación de modelos de prevención de riesgos es la

"PRÁCTICAMENTE TODOS LOS EMPRESARIOS ENTIENDEN QUE EL *COMPLIANCE* GENERA CREDIBILIDAD Y CONFIANZA"

proporcionalidad y cuenta con ventajas como la protección frente a la responsabilidad personal de los administradores; la mejora en la gestión; la satisfacción de empleados, proveedores, clientes, y otras partes interesadas, etc. Los administradores de una pyme deben efectuar un análisis de acuerdo con sus propias exigencias de organización y gestión, de modo que busquen y encuentren el punto de equilibrio entre la reducción de costes de cumplimiento y la mejora de los controles.

¿Los cambios normativos y regulatorios suponen nuevos riesgos para las compañías?

Desde la perspectiva del *compliance*, más que cambios normativos y regulatorios que impliquen nuevos riesgos, lo que es evidente es que estamos ante un mundo completamente globalizado e hiperconectado y que la Covid-19 ha acelerado esta situación. Existen muchas normas y directivas internacionales, especialmente a nivel comunitario, que pretenden regular la realidad y el entorno económico y de negocios que estamos viendo. La tendencia se dirige a regular todos los ámbitos de las relaciones comerciales y empresariales para garantizar una manera de hacer negocios transparente y ética que dote de mayor seguridad jurídica y credibilidad al mercado y a sus operadores. Por tanto, más que nuevos riesgos, lo que proliferan son nuevas normas y obligaciones que las organizaciones están obligadas a cumplir en el ejercicio de su actividad, lo que exige seguir destinando recursos

y esfuerzo al *compliance*. Específicamente en materia de *compliance*, España debe transponer antes del 17 de diciembre de 2021 la Directiva (UE) 2019/1937 del Parlamento Europeo y del Consejo, de 23 de octubre de 2019, relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión (en inglés, conocida coloquialmente por *whistleblowers* o denunciantes). La implantación del *whistleblowing* o canal de denuncias interno es una pieza clave en la implantación de un modelo efectivo de *compliance* penal para evitar responsabilidades penales de las personas jurídicas en los ámbitos laborales o financieros. Sin embargo, los denunciantes potenciales suelen renunciar a informar sobre sus preocupaciones o sospechas por temor a represalias por la "cultura del chivatazo", y los canales de denuncia no se utilizan todo lo deseable para asegurar la eficacia de los Modelos. En este contexto, es cada vez mayor el reconocimiento de la importancia de prestar una protección equilibrada y efectiva a los denunciantes. Las líneas de denuncia han de cumplir requisitos como: garantías de confidencialidad y tramitación diligente; acuse de recibo; el establecimiento de unos plazos concretos y razonables o la designación de personas imparciales para tramitar las denuncias.

Ciberseguridad y protección de datos corporativos, ¿cómo ha cambiado la digitalización la función de *compliance*?

Toda organización o profesional que almacene o trate datos de carácter personal de terceros, o que los haga susceptibles de tratamiento, tendrá que cumplir con las formalidades exigidas en el Reglamento General de Protección de Datos (RGPD) y la Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD), bajo amenaza de sanciones en caso de incumplir las obligaciones expuestas en dicha normativa. El concepto clave en materia de protección de datos es, como ocurre en materia de *compliance* penal, el de accountability o responsabilidad. Este concepto exige al empresario un deber de diligencia respecto de los datos que almacena y trata. Tiene la obligación de identificar en qué procesos son tratados esos datos de carácter personal de terceros y de confeccionar un mapa de riesgos, que establezca prioridades en el tratamiento de los datos y defina controles adecuados a los riesgos detectados. Desde el punto de vista de prevención del riesgo y, precisamente como consecuencia de la pandemia del Covid-19, la velocidad a la que los negocios se está digitalizando es directamente proporcional a los riesgos asociados a esta nueva realidad (teletrabajo, conexión desde dispositivos personales, wifis inseguras, e-commerce, etc.). Por este motivo, hoy día la protección de datos tiene que estar coordinada con un buen plan de ciberseguridad. Los planes de acción ante ciberataques tienen una estructura muy similar al *compliance* penal y tienen que permitir a las organizaciones tener capacidad de prevención, detección, respuesta y recuperación.

¿La pandemia ha acelerado la implantación de modelos de ciberseguridad?

La pandemia ha despertado al monstruo virtual. En un mundo hiperconectado, la ciberseguridad está en peligro. Estamos más expuestos que nunca. Los ataques en la red son cada vez más agresivos, y en España han llegado a poner en jaque infraestructuras del Estado. Internet es el campo de batalla donde delincuentes y terroristas desafían y manipulan a Gobiernos, ciudadanos y empresas. La red no fue concebida hace 30 años como un lugar seguro. Y nadie ha ejercido nunca sobre ella su soberanía. Es global, abierta, rápida, dinámica, de fácil acceso, con una enorme capacidad de anonimato y escasamente regulada. En ella está la información, los servicios, las ideas... Nuestros datos. Y tampoco son seguros los sistemas informáticos que utilizamos. No han sido concebidos bajo parámetros de ciberseguridad. Y aunque esté blindado el sistema de una infraestructura crítica (un aeropuerto, una refinería, un hospital...), pueden no estarlo las empresas que prestan servicios, sus proveedores, socios y subcontratistas, los encargados del mantenimiento o sus empleados. Los ataques cibernéticos son cada vez más sofisticados. Con el inicio de la aplicación del RGPD en 2018 los costes derivados de las infracciones en materia de protección de datos se han disparado (las multas pueden llegar a ser de hasta 20 millones de euros o el 4 % del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la mayor cuantía). Pero el coste no es solo económico, sino también reputacional, siendo precisamente la pérdida de credibilidad y confianza del resto de operadores del mercado el coste más elevado de no adoptar las medidas de control adecuadas.

¿Cuáles son las perspectivas de crecimiento de Ontier?

Tras más de diez años desarrollando su expansión internacional, el objetivo de Ontier es seguir consolidando y reforzando sus capacidades en los 13 países en los que está presente. Principalmente, en Latinoamérica, donde somos la firma internacional con mayor presencia, con oficinas en nueve países, además de Italia, Reino Unido y España. Nuestro objetivo a nivel global es ser la firma de referencia para aquellas empresas que tengan intereses en el mercado latinoamericano. ◆