El uso y seguimiento de la tecnología por los responsables de cumplimiento normativo

En un contexto de intensa transformación digital, se ha celebrado la Semana Internacional del Compliance

Entre los días 15 y 19 de noviembre se ha celebrado la Semana Internacional del Compliance, organizada por la WCA (World Compliance Association), CUMPLEN (Asociación de profesionales de Cumplimiento Normativo) y el IOC (Instituto Oficiales de Cumplimiento. En un contexto de intensa transformación digital impulsada por la pandemia, la tecnología ha sido también protagonista de las charlas de expertos, talleres y ponencias del curso perito compliance. Por una parte, porque cada vez resulta más clara la necesidad de estos profesionales de contar con herramientas tecnológicas para el desempeño de sus funciones. Por otro, porque el propio desarrollo de determinadas tecnologías requiere el enfoque de riesgos propio del compliance.

Enfoque de los riesgos

Antonio Muñoz Marcos, director, global DPO Office en Telefónica, ha sido el responsable de la última charla del congreso, dedicada a inteligencia artificial y compliance. El experto ha puesto el acento en las líneas maestras de la regulación de la inteligencia artificial por la Comisión Europea, a través del borrador de reglamento publicado en primavera de este año 2021. Desde la perspectiva del compliance, ha explicado los tres tipos de riesgos que pueden aparecer en proyectos que usen esta tecnología: inaceptables, altos o bajos. Los primeros ocupan gran parte de la norma, y suponen que el sistema resulte prohibido. No obstante, se prevé su posible uso ante amenazas inminentes, con la consiguiente duda de cómo podrá pasar a utilizarse algo que estaba previamente vedado, por ejemplo, el reconocimiento facial en espacios públicos.

En todo caso, el desarrollo de sistemas que usen esta tecnología, obligatoriamente va a utilizar modelos de cumplimiento orientados al riesgo, con seguimiento posterior a la comercialización, pues precisamente las tecnologías que usan inteligencia artificial no se culminan cuando se saca al mercado, sino que necesitan todo un ecosistema de gestión de calidad también después, con una jerga que resulta muy familiar a los responsables de cumplimiento normativo. Ha incidido en el necesario cuidado que ha de tenerse con la normativa de protección de los datos usados en herramientas de inteligencia artificial, así como con los sesgos a la hora de elaborar los algoritmos y el cuidado al abordar su preceptiva explicabilidad.

IA aplicada al cumplimiento normativo

Álvaro Écija, socio director de Écix, ha impartido una charla experta con un ejemplo práctico sobre cómo la inteligencia artificial puede ayudar a detectar brechas legales a través de la combinación de dos diciplinas: estadísticas matemáticas y machine learning. “¿Se pueden poner números a los incumplimientos?”, ha planteado. Pasando a responder que “sí, porque hay sanciones económicas”, de modo que es posible usar un algoritmo que parte de la ecuación según la cual el valor del riesgo legal es igual al producto del impacto por la probabilidad de que ocurra; obteniendo la probabilidad mediante la multiplicación de la amenaza (o factor externo), por la vulnerabilidad (o factor interno).

Ha indicado que se puede asignar una cuantía a la amenaza a través de la organización en tablas de los datos numéricos que arrojan las resoluciones sancionadoras. Para la vulnerabilidad se precisaría un análisis de la información de la organización, a través de un sistema sustentado en machine learning. Es la metodología que usa la solución que su equipo ha preparado, en colaboración con la Universidad Complutense. Un producto denominado “Mia”, que ayuda a los compliance officers en las tres fases de su función: diagnóstico, análisis de riesgos y fase de decisión o “soluciones legales”; y en diferentes campos de cumplimiento normativo (medio ambiente, penal, protección de datos, blaqueo de capitales, etc.)

Blockchain e identidad digital

La anteúltima charla del congreso, “La tecnología aplicada en las tres líneas de defensa”, ha corrido a cargo de **María Dolores Pescador** , executive chairman en Logalty, quien ha impartido una ponencia en la que ha aludido a muchas otras tecnologías al servicio del cumplimiento normativo.

Así, ha incidido en la relevancia de las notificaciones electrónicas con firma digital, mostrando diferentes casos de uso en los que puede ser relevante, sobre todo para demostrar la validez de contratos celebrados de manera electrónica o telefónica. Ha explicado el sistema que usan en su organización, Logalty, generando prueba con apoyo en matriz distribuida, mediante tecnologías blockchain, con entrega del hashtag a cinco notarios diferentes; y también el modelo de funcionamiento de su hub de comunicaciones, personalizable por sus clientes.

Pescador ha señalado la relevancia de la identidad digital, constatando un crecimiento en su importancia y uso. “La contratación apoyada en la tecnología, con plena seguridad jurídica, es el futuro inmediato”, ha dicho, refiriéndose a la situación tras la pandemia. Por ello, ha incidido en la importancia estratégica del gobierno y control de los riesgos técnicos a través de auditorías con comprobaciones que cuentan con hackers éticos.

Sistemas para la gestión de riesgos

También en la charla sobre Compliance & Ethics All In, la jefa de la División de Gobierno Corporativo y Cumplimiento AENA, **Ana Luisa Zuleta Pérez de Guzmán**, al mencionar el mapa de riesgos en una organización tan compleja como la suya, con riesgos muy variados, ha incidido en la necesidad de contar con un sistema integrado, una herramienta que centralice los riesgos y controles, por ser útil para la compañía y eficiente para el cumplimiento. “Hay que procurar que los riesgos sean conocidos y que los sistemas de control integrado tengan en cuenta todo. Hay que evitar que haya sistemas de control repetidos que no se hablen y no casen”, ha dicho.

Sobre ello ha incidido también María Dolores Pescador, de Logalty, cuando comentó, con respecto a los informes de los distintos niveles de reporting, el requisito de que obtener informes del pasado debe ser “tan sencillo como dar a un botón” en la herramienta que se utilice. Ha señalado que se trata, junto con la monitorización continua, de una cuestión “muy importante para el compliance.

Canal de denuncias

Dentro del Curso Perito Compliance, **Cristina Fabre Chicano**, consejera IOC y directora de Auditoría, Cumplimiento y Riesgos de CEPSA, ha explicado las reglas sobre protección de alertadores que recoge la Directiva Whistleblowing, cuyo plazo de transposición es inminente: el próximo 17 de diciembre. Ha explicado los pasos que recoge dicha norma, así como las vías para proteger al alertador, pero también al “denunciado”. También ha advertido de algunas implicaciones laborales en los plazos de respuesta cuando la denuncia se dirija contra un empleado. Y ha señalado la necesidad de divulgar el canal y contar con indicadores claros, como por ejemplo el número de denuncias que se pueden esperar en función del número de trabajadores. En cuestión de tecnología, ha aconsejado contar con alguna de las herramientas disponibles en el mercado, con gestión del proceso end to end, al día de la refomas normativas y fiable en cuestiones de seguridad. “Tener una herramienta ayuda mucho en la gestión del canal”, ha dicho.

En el mismo sentido se ha pronunciado María Dolores Pescador al referirse a la que comercializa su organización como “un arma muy potente” en la lucha contra las malas prácticas y la corrupción.

En definitiva, sea desde la perspectiva de usuarios de herramientas que aligeran su labor, sea desde el punto de vista del control del cumplimiento normativo en el desarrollo de sistemas que utilizan tecnologías como las empleadas por la inteligencia artificial, también en el perfil de los compliance officers, se muestra cada vez más relevante la evolución digital.

Fuente: Cinco Días