La doble cara de los algoritmos en la era del ’compliance’

La IA puede transformarse en un útil aliado ante la avalancha normativa, pero también en un nuevo territorio de riesgo que exige gobernanzas sólidas

El desempeño del cumplimiento normativo, del 'compliance', incumbe cada vez más a los departamentos y proveedores de tecnología de las empresas, que no deben desviarse del eficiente alineamiento con los rigores de la transformación digital y la responsabilidad social. De hecho, el 'Libro Blanco de la Función de Compliance' elaborado por Ascom (Asociación Española de Compliance) destaca la importancia de la tecnología (con especial foco en la IA) de cara «al control de riesgos (crisis internas o de reputación) y a la planificación de estrategias», con atención, además, a procesos como la ciberseguridad, la privacidad de datos o la trazabilidad de los procesos.

La actualidad en este ámbito ha pasado por la reciente celebración de dos eventos organizados por World Compliance Association (WCA), la principal asociación de profesionales del cumplimiento normativo en habla hispana: SIC-Somos Integridad y Cumplimiento y la Compliance & Tech Summit 2025, foros en los que se ha abordado esta cuestión clave para las empresas y la sociedad. Como destaca el director general de la WCA, José Luis Casero: «Creemos en un humanismo tecnológico en el que la IA, la digitalización y la automatización están transformando el papel de los profesionales del compliance».

Reto gigantesco

«Más allá de mejorar tareas técnicas (continúa Casero), la IA redefine la profesión al exigir combinar dominio legal, comprensión tecnológica, sensibilidad ética e inteligencia emocional. Creemos que el valor del profesional radica en interpretar y contextualizar los resultados algorítmicos, tomando decisiones justas, prudentes y responsables, velando por la dignidad humana frente a decisiones técnicas automatizadas». Sin olvidar además «que la tecnología democratiza procesos y potencia la función consultiva, pero siempre con la persona en el centro». Un enfoque que supone todo un desafío ante la inmensidad de datos sensibles, ante los que la IA colabora en tareas como la revisión de 'frameworks', controles automatizados, obligaciones en gestión, en cifrado etc.

Las distintas ponencias de los mencionados foros aportaron reflexiones sobre la doble cara (esperanzadora por una parte; con prevención, por otra) de esta excepcional irrupción tecnológica que sustentan opiniones como la de Iván Martínez CEO de Intedya: «La IA ha dejado de ser una cuestión meramente tecnológica para convertirse en un asunto de gobierno corporativo y cumplimiento normativo. La nueva regulación europea, a través del EU AI Act, introduce obligaciones claras de evaluación de riesgos, transparencia, control y supervisión de los sistemas de IA, así como cuantiosas sanciones por incumplimiento de los marcos exigibles de control a las empresas, con marcos internacionales como la norma ISO 42001, un modelo práctico y auditable para integrar estas exigencias en las organizaciones».

Riesgos crecientes

Potencia bajo control sobre la que Martínez añade la importancia de «la creación de nuevos perfiles como el AI Officer, responsable de coordinar riesgos, ética y 'compliance' en el uso de la IA. Las organizaciones que no gobiernen adecuadamente la IA se exponen a riesgos legales, reputacionales y operativos crecientes. La IA ya no es solo una ventaja competitiva, sino una responsabilidad que exige estructuras, roles y controles claros». Hay que estar, sin duda, muy finos para identificar riesgos, prevenir incumplimientos, reforzar los controles internos «con soluciones (concluye Martínez) que analizan grandes volúmenes de datos para detectar anomalías, posibles fraudes o conflictos de interés, así como sistemas que apoyan la evaluación de proveedores, la gestión de denuncias o el seguimiento de obligaciones normativas. La clave no está en usar más tecnología, sino en integrar la IA dentro de un marco de 'compliance' sólido, con supervisión humana, criterios claros y responsabilidad».

En esta unión de disrupción tecnológica y sentido común (con permiso de las complejidades propias de la tozuda realidad), la proactividad cotiza al alza, como han demostrado compañías de alcance global como IBM. Esta firma ha desarrollado IBM Guardium para proteger datos sensibles en entornos locales, cloud o híbridos, permitiendo monitorizar accesos en tiempo real, detectar actividades inusuales y automatizar respuestas ante posibles brechas. Proactividad, y prevención, tan necesarias como subraya Vanessa Fernández Lledó, socia del área Penal Económico e Investigaciones Internas y directora de Corporate Compliance de Gómez-Acebo & Pombo Abogados: «El uso de herramientas de IA supone una mejora evidente para la detección y prevención de conductas irregulares dentro de las compañías, pero no sustituye la supervisión por parte de los 'compliance officers' internos y asesores externos».

Habrá que tener, por lo tanto, un especial cuidado a la hora del uso y obtención de información, ya que, como considera Fernández Lledó: «Puede colisionar con derechos fundamentales (intimidad, protección de datos, etc.) y garantías procesales. La laguna legal sobre su uso y alcance contribuye a ello (una vez más, la tecnología va por delante de la legislación). Será necesario implementar políticas de respeto a los principios de necesidad, idoneidad y proporcionalidad en cuanto al uso por la empresa de la IA, y los controles deberán ajustarse a la legislación vigente, incorporando criterios de transparencia y limitación».

Vigilar el escudo digital

Antonio Hernández-Briz, enterprise account director de Formalize y Carlos Saiz, vicepresidente de Ecix, participaron en un diálogo sobre ciberseguridad en el marco de SIC 2025. Como se destacó en el encuentro, este aspecto es un vector clave «para proteger nuestra vida privada, la infraestructura crítica y la continuidad de empresas y servicios públicos»… tanto, que como se destacaba en estudios como los publicados por 'IT Governance', en 2024, más de 35.000 millones de registros estuvieron expuestos ante cerca de 9.500 incidentes. En este entorno, regulaciones como la Directiva NIS2 (hará solidariamente responsables a los órganos de dirección), implica una mayor conciencia sobre la inapelable madurez en materia de ciberseguridad.

Olga Fraga Gómez, socia Ethics & Compliance de Deloitte Legal, coincide en la relevancia de equilibrar posibilidades de desarrollo con riesgos: «La IA es una palanca de expansión de negocio y de eficiencia para nuestras empresas, pero también un nuevo territorio de riesgo que exige gobernanza. Estamos viendo cómo los equipos de 'compliance' pasan de ser reactivos a predictivos, usando la IA para anticipar conductas, fraudes o incumplimientos y para comunicar mejor». La especialista confía en un futuro en el que el compliance «sea el garante de una IA confiable, alineada con valores, regulación y propósito empresarial. Las organizaciones que así lo entienden ya están cumpliendo mejor pero, sobre todo, competirán mejor».

Jorge Cabet, managing partner de Cabet Abogados, indica la paradoja de la existencia «de una pescadilla que se muerde la cola: los textos que produce la IA y la información de la que se alimenta… se genera mucha información que nadie lee realmente, con la que se nutre de nuevo el sistema de IA y la calidad se hunde, amplificando un problema que puede generarnos este nuevo año abundantes alucinaciones y problemas crecientes con documentos francamente defectuosos». La 'diligencia de revisión documental' y, siempre, la formación actualizada forman parte del kit para afrontar esta avalancha tecnológica, aún más cuando «es posible que este año los propios proveedores de LLM's se enfrenten a mayor presión por sus outputs puesto que los escándalos en el uso de la IA escalarán».

'Alucinaciones'

Desde el punto de vista de las asociaciones sectoriales, Justo Hidalgo, director de Inteligencia Artificial de Adigital, subraya cómo ya se disfruta de las ventajas de sistemas «que monitorizan cambios normativos casi a tiempo real y alertan sobre impactos específicos en políticas internas, herramientas de análisis contractual que detectan cláusulas potencialmente problemáticas desde la óptica de protección de datos, competencia o consumo, o asistentes que ayudan a documentar evidencias de diligencia debida exigidas». Justo Hidalgo avisa también sobre la importancia del correcto balance entre fuentes jurídicas utilizadas confiables, legislación referenciada vigente e información proporcionada con estándares de calidad: «Así se podrán evitar los sesgos y las 'alucinaciones', o una falsa sensación de cumplimiento por exceso de automatización, una falta de rigor y responsabilidad inadmisible en el ámbito del cumplimiento normativo y regulatorio».

Un recorrido, en suma, en el que desde Gómez-Acebo & Pombo Abogados, insisten (en este caso, Enrique Luzón Campos, counsel del área Penal Económico e Investigaciones Internas) en que «la IA también es una herramienta que puede ser utilizada por aquellos que quieren incumplir las normas internas, o incluso cometer delitos, por lo que supone un nuevo desafío para las compañías en materia de cumplimiento y prevención interna».

Fuente: https://www.abc.es/

LINK DE LA NOTICIA