

El impacto del paquete ómnibus digital europeo en los sistemas de ‘cybercompliance’

Cada ajuste normativo exige revisar políticas, controles, responsabilidades, indicadores y, sobre todo, mapa de riesgos

La Unión Europea parece haber encontrado en la palabra ómnibus una solución para un problema que ella misma ha creado: la acumulación de normas digitales. El llamado paquete ómnibus digital, con propuestas de simplificación, ajustes y alineamientos del acervo existente, llega en un contexto complejo. Por un lado, las empresas respiran ante la promesa de reducir cargas. Por otro, los responsables de cumplimiento, DPO’s, directores legales y CISO’s miran sus sistemas y se preguntan cómo abordar, una vez más, cambios normativos que no solo afectan a lo jurídico, sino a la esencia de la gestión del riesgo tecnológico.

Gran parte del debate público se ha centrado en los impactos legales del ómnibus digital: qué se deroga, qué se modifica y qué se retrasa. Pero se habla mucho menos del impacto directo sobre los sistemas de gestión de cumplimiento. Y ahí es donde muchas organizaciones se juegan el éxito o el fracaso de su estrategia regulatoria.

No estamos ante un fenómeno aislado. RGPD, NIS2, DORA, CRA, Reglamento de IA, Data Act… el conjunto normativo digital europeo se ha convertido en un auténtico ecosistema. El paquete ómnibus no reduce esta complejidad de forma automática; en muchos casos, la redistribuye. Simplificar normas no significa necesariamente simplificar el cumplimiento, al menos en el corto plazo.

Desde el punto de vista de cybercompliance, cada ajuste normativo exige revisar políticas, controles, responsabilidades, indicadores y, sobre todo, mapa de riesgos. El problema no es solo jurídico: es organizativo, tecnológico y presupuestario.

La mayoría de las empresas, especialmente medianas, no cuentan con equipos ni presupuestos infinitos. Pretender implementar sistemas de cumplimiento “perfectos” para cada nueva norma es una tarea inviable. Aquí es donde el enfoque debe cambiar, del cumplimiento normativo fragmentado a la gestión integrada del riesgo digital. La pregunta clave no es “¿cómo cumplo con todo?”, sino “¿dónde debo poner el foco ahora?”. En momentos de incertidumbre regulatoria, la priorización es una decisión estratégica.

Un error frecuente es construir sistemas de cumplimiento basados en listas de obligaciones legales. En contextos normativos complejos, este tipo de sistemas empiezan a mostrar sus carencias porque se desactualizan rápido y difícilmente incorporan matices propios de normativas basadas en principios. Un sistema de cybercompliance robusto debe partir de riesgos transversales: interrupción operativa, pérdida de datos, fallos de gobernanza algorítmica, dependencia crítica de terceros tecnológicos, sanciones regulatorias acumuladas o daño reputacional.

El paquete ómnibus digital no elimina estos riesgos; los reconfigura. Por eso, más que rehacer todo el sistema, conviene revisar si el mapa de riesgos sigue siendo válido y si los controles existentes siguen mitigando los riesgos más críticos.

La tentación de unificar sistemas de gestión es comprensible: menos procesos, menos auditorías, menos fricción interna. Pero la unificación mal entendida puede diluir matices esenciales. No es lo mismo gestionar riesgos de ciberseguridad que riesgos derivados del uso de IA o del intercambio de datos concretos.

La clave está en un modelo híbrido: un núcleo común de gobernanza, metodología de riesgos y reporting, combinado con capas específicas por dominio regulatorio. Un marco compartido que permita tratar de forma coherente obligaciones muy distintas sin diluir sus particularidades técnicas. En este punto, los estándares internacionales de sistemas de gestión de cumplimiento, como ISO 37301, pueden aportar una estructura útil: no dictan qué norma cumplir, sino cómo organizar el cumplimiento en entornos normativos complejos.

Si algo ha demostrado la regulación digital europea es que no es estática. Guías, dictámenes, criterios de autoridades y ahora paquetes ómnibus obligan a pensar el cumplimiento como un proceso vivo. Los sistemas rígidos, basados en checklists anuales, están condenados a quedarse obsoletos. Un buen sistema de cybercompliance debe incorporar mecanismos de revisión continua, un observatorio regulatorio (incluyendo criterios interpretativos) y ciclos cortos de actualización de riesgos y controles. No se trata de rehacerlo todo cada vez, sino de poder ajustar elementos con agilidad.

En este contexto, la tecnología deja de ser un accesorio y se convierte en un habilitador clave. Plataformas de GRC, automatización de evidencias, gestión centralizada de terceros o analítica de riesgos permiten absorber parte de la creciente carga burocrática asociada a este ecosistema regulatorio. En particular, el uso responsable de herramientas de inteligencia artificial puede ayudar a clasificar obligaciones, mapear impactos normativos o priorizar riesgos, siempre que se integren bajo criterios de gobernanza claros y con supervisión humana efectiva.

En conclusión, el paquete ómnibus digital debería servir como recordatorio de que el verdadero reto no es entender la norma, sino gobernar su impacto. Las empresas que inviertan ahora en sistemas de cybercompliance integrados, flexibles y orientados al riesgo estarán mejor preparadas no solo para cumplir, sino para competir en una Europa cada vez más regulada. Porque, al final, el cumplimiento ya no es solo una obligación legal, es una capacidad estratégica.

Fuente: https://cincodias.elpais.com/

LINK DE LA NOTICIA