



De la carga burocrática a la ventaja competitiva: cómo prepararse para los nuevos retos regulatorios de la economía digital

La transformación digital de las empresas ya no depende únicamente de la incorporación de nuevas tecnologías. Cada vez más, el éxito de una estrategia digital está ligado a la capacidad de anticiparse y adaptarse a un marco normativo en constante evolución.

Con el objetivo de ayudar a las empresas a comprender este nuevo escenario, la Oficina Acelera Pyme de FADE celebró la jornada **“Novedades y retos regulatorios en la economía digital: de carga burocrática a palanca de negocio”**, en colaboración con Garrigues. Durante la sesión, expertos en economía del dato, privacidad, ciberseguridad y relaciones laborales analizaron las principales novedades regulatorias que marcarán los próximos años y su impacto práctico en la actividad empresarial.

El Reglamento Europeo de Inteligencia Artificial: el punto de partida

Uno de los mensajes clave de la jornada fue que las organizaciones deben comenzar cuanto antes a prepararse para la aplicación del Reglamento Europeo de Inteligencia Artificial (AI Act).

Los especialistas de Garrigues destacaron que el primer paso consiste en identificar qué sistemas de inteligencia artificial utiliza realmente la organización. Para ello, resulta imprescindible realizar un inventario de sistemas de IA y determinar cuáles entran dentro de la definición regulatoria de inteligencia artificial y cuáles quedan excluidos.

A partir de ahí, las empresas deben clasificar los sistemas empleados según el nivel de riesgo definido por la normativa: sistemas prohibidos, sistemas de alto riesgo, sistemas de riesgo limitado y sistemas de riesgo mínimo o nulo. También cobrará especial relevancia la regulación de los modelos de IA de propósito general (GPAI) y de los sistemas de IA agéntica.

Identificar responsabilidades y nuevas obligaciones

La regulación no afecta únicamente a quienes desarrollan tecnología. Dependiendo de su papel, las organizaciones pueden asumir distintos roles: proveedor, responsable del despliegue (usuario), distribuidor, importador o representante autorizado.

Cada uno de estos roles implica diferentes obligaciones de cumplimiento. Entre ellas destacan requisitos relacionados con la transparencia, la alfabetización en inteligencia artificial, la documentación técnica o la supervisión de los sistemas utilizados.

En el caso de los sistemas de alto riesgo, las obligaciones son especialmente exigentes e incluyen aspectos como la gestión de riesgos, la gobernanza de datos, la supervisión humana, la ciberseguridad, la evaluación de conformidad o la notificación de incidentes graves.

Además, determinadas aplicaciones deberán informar expresamente cuando una persona esté interactuando con un sistema de IA o cuando el contenido haya sido generado artificialmente, un aspecto especialmente relevante ante la creciente proliferación de contenidos sintéticos y deepfakes.

IA, privacidad y ciberseguridad: tres ámbitos inseparables

Otro de los ejes de la jornada fue la estrecha relación existente entre inteligencia artificial, protección de datos y ciberseguridad.

La implantación de sistemas de IA obliga a revisar aspectos relacionados con la legitimación de tratamientos automatizados, la transparencia hacia usuarios y clientes, las transferencias internacionales de datos y las medidas de seguridad exigibles en cada caso.

Los ponentes recordaron que las empresas deberán afrontar un entorno regulatorio cada vez más integrado, donde convivirán normas como el Reglamento General de Protección de Datos (RGPD), la Directiva NIS2, el Reglamento de Inteligencia Artificial, el Reglamento de Resiliencia Cibernética (Cyber Resilience Act), DORA o el Esquema Nacional de Seguridad.

Hacia una simplificación del marco regulatorio europeo

La Comisión Europea trabaja actualmente en distintas iniciativas orientadas a simplificar y armonizar el ecosistema normativo digital.

Durante la jornada se analizaron las propuestas incluidas en el denominado Reglamento Ómnibus Digital, que contempla medidas para simplificar determinadas obligaciones relacionadas con la IA, impulsar la alfabetización digital, facilitar el tratamiento de ciertos datos para evitar sesgos en sistemas de

alto riesgo y reforzar la lucha contra prácticas especialmente sensibles como los deepfakes maliciosos.

Asimismo, se expusieron las modificaciones previstas en la regulación de datos y ciberseguridad. Entre ellas destacan iniciativas para unificar normas de gobernanza de datos y reutilización de información pública, así como la creación de modelos únicos de notificación de incidentes de seguridad y sistemas de “ventanilla única” para facilitar el cumplimiento empresarial.

El impacto de la IA en las relaciones laborales

La segunda parte de la jornada estuvo centrada en el efecto de la inteligencia artificial sobre las relaciones laborales.

Los expertos recordaron que el Reglamento Europeo de IA considera de alto riesgo determinados sistemas utilizados en ámbitos como la contratación, la evaluación de trabajadores, la promoción profesional o la gestión del desempeño. Como consecuencia, las organizaciones deberán garantizar mecanismos de supervisión humana y proporcionar información a las personas trabajadoras y a sus representantes cuando se utilicen este tipo de herramientas.

Además, tanto el RGPD como el Estatuto de los Trabajadores reconocen derechos específicos relacionados con las decisiones automatizadas y con la utilización de algoritmos que puedan influir en las condiciones de trabajo, el acceso o el mantenimiento del empleo.

La justicia ya está marcando el camino

La ponencia repasó también varias resoluciones judiciales recientes relacionadas con el uso de algoritmos e inteligencia artificial en el ámbito laboral.

Los tribunales están comenzando a exigir mayores niveles de transparencia en los sistemas automatizados utilizados por las empresas y a reforzar la obligación de informar a la representación legal de los trabajadores sobre los parámetros y criterios utilizados por estos sistemas. Asimismo, se destacó la importancia de mantener siempre mecanismos efectivos de supervisión humana para evitar riesgos de discriminación o vulneración de derechos fundamentales.

Una oportunidad para las empresas

La principal conclusión de la jornada fue clara: la regulación digital no debe entenderse únicamente como una obligación administrativa.

Las empresas que sean capaces de incorporar de forma temprana principios de gobernanza de datos, inteligencia artificial responsable, privacidad y ciberseguridad estarán en mejor posición para generar confianza, reducir riesgos y aprovechar nuevas oportunidades de negocio.

En un contexto donde la innovación y la regulación avanzan cada vez más unidas, anticiparse al cumplimiento normativo puede convertirse en una auténtica ventaja competitiva.

