La regulación europea a grandes tecnológicas transforma la economía digital

La regulación en tecnología de la Unión Europea constituye un éxito que ésta empezando a equilibrar las condiciones de competencia entre los gigantes de Sillicon Valley y sus rivales en Europa, de acuerdo con la comisaria europea de Competencia, Teresa Ribera.

De acuerdo con la funcionaria europea, la Ley de Mercados Digitales de la UE ha impulsado cambios en el funcionamiento de la economía digital europea desde 2023, cuando la Comisión comenzó con la aplicación de este marco de normas en competencia digital. “Los dos objetivos principales para garantizar la igualdad de condiciones en los mercados digitales son asegurar la interoperabilidad -para que los usuarios tengan libertad de elección- y el acceso a los datos”, afirmó Ribera. Esto ha mejorado significativamente en los últimos años en lo que respecta al uso de teléfonos, servicios, el acceso a las plataformas y a los datos.

Las declaraciones de la comisaria se producen en un momento en que Bruselas se prepara para llevar a cabo una revisión formal de la Ley de Mercados Digitales para determinar qué aspectos funcionan y en que puntos sería necesaria reformar la ley. La reglamentación busca impedir que las empresas “guardianas”, utilicen su posición dominante para limitar la competencia de jugadores más pequeños.

Ribera rechazó las críticas por parte de organizaciones de la sociedad civil y terceros con respecto a la aplicación de la legislación en la investigación a Google sobre la configuración de su página de búsquedas, argumentando que el “Estado de derecho” exige un enfoque metódico basado en pruebas y en el debido proceso.

Regulación emergente

El gobierno australiano presentó un proyecto de ley que solicitaría a las empresas de tecnología incluidas Meta, Google y TikTok pagar por el periodismo que compartan en sus plataformas, o de lo contrario, afrontar el pago de un impuesto sobre sus ingresos locales. La legislación propuesta, the *News Bargaining Incentive*, impondría un impuesto de 2.25% a los ingresos australianos de las tres plataformas a menos que lleguen a acuerdos con editores de noticias locales. Entre más acuerdos concreten con los medios, menor sería la tasa impositiva, permitiendo la generación de entre 200 y 250 millones de dólares australianos para el periodismo local.

La Comisión Europea (CE) buscaría ampliar el alcance de la Ley de Mercados Digitales a los servicios en la nube y de inteligencia artificial con el objetivo de promover una competencia más justa en estos sectores digitales. Esta ley impone obligaciones a empresas como Alphabet, Amazon, Booking, ByteDance y otros, para evitar que abusen de su posición dominante en el mercado. “La Ley de Mercados Digitales se diseñó para estar preparada para nuevos retos, como la inteligencia artificial y la nube”, comentó la responsable en competencia de la Unión Europea en un comunicado oficial.

Datos y negocios digitales

Automatización en construcción de centros de datos

La multinacional SoftBank planea el desarrollo de una nueva firma para automatizar la creación de estructura de centros de datos. RozeAI, el nombre de esta empresa trabajaría en la construcción eficiente de centros de procesamiento en los Estados Unidos con el apoyo de robots autónomos. El conglomerado ya prepara a RozeAI para su ingreso a la bolsa y ejecutivos buscan que se produzca en el segundo semestre de 2026. La valoración prevista podría ser de 100 mil millones de dólares.

Aerolínea japonesa pone a prueba robots humanoides

Japan Airlines comenzó a probar robots humanoides en sus operaciones en tierra en el aeropuerto de Haneda, en Tokio, debido a la escasez de mano de obra. La aerolínea se asoció con GMO AI & Robotics para poner a prueba robots destinados a tareas de carga de equipaje y limpieza de cabina. La iniciativa surge en un momento en que el sector de la aviación japonés se enfrenta al aumento de demanda turística y una caída en mano de obra, provocado, principalmente por el envejecimiento de su población.

Riesgos de seguridad

Hackers Iraníes atacan infraestructuras críticas de Estados Unidos

En medio de los conflictos entre Estados Unidos e Irán, hackers afiliados al gobierno iraní llevaron a cabo un ataque contra los sistemas de control industrial en todo Estados Unidos, incluidos los servicios públicos de energía y agua. El FBI y la Agencia de Seguridad Nacional entre otras instancias mencionaron que los hackers atacaron los dispositivos diseñados para permitir el control digital de maquinaria física, cambiando la información de las pantallas de los sistemas industriales. El comunicado de las agencias no especifica un grupo responsable, sin embargo, señala que son similares a los llevados a cabo por el grupo CyberAv3ngers, el cual está vinculado con Irán.

Hackers chinos, atacan desde lo cotidiano hasta sectores críticos

El Centro Nacional de ciberseguridad de Gran Bretaña (NCSC) en conjunto con diversas agencias, como el FBI y 15 socios internacionales de ocho países diferentes, publicó nuevas directrices que advierten sobre grupos de ciberataque chinos que suelen infiltrarse, mediante redes encubiertas, a dispositivos de uso cotidiano conectados a internet, como enrutadores domésticos y dispositivos inteligentes, los cuales utilizan como el primer paso para atacar sectores críticos a nivel mundial, robar datos confidenciales y lograr un acceso persistente. Los ataques pueden ser difíciles de detectar ya que las pruebas pueden desaparecer rápidamente, complicando la detección de esta actividad.

Digitalización e Infraestructura

Orbital y SpaceX planean realizar la primera misión para instalar centros de datos de inteligencia artificial en órbita terrestre en 2027. El proyecto busca aprovechar la energía solar constante y la refrigeración natural del espacio. Aunque SpaceX reconoce que los centros de datos en la órbita pueden operar en un entorno hostil e impredecible, incluso provocando riesgos y fallos al enfrentarse a las condiciones del espacio, ya se encuentran trabajando en la infraestructura y legislación adecuada para un mejor y óptimo desarrollo.

Food for thought

Los ataques cibernéticos en la industria manufacturera han crecido exponencialmente, según señala el informe Manufacturing Threat Landscape de Check Point, una empresa global de ciberseguridad. El estudio señala que los incidentes de ransomware aumentaron 56% en 2025, escalando de 937 a 1,466 casos. Dentro de este panorama, América Latina se posicionó como la región más atacada del mundo en 2025, con un promedio de 3,054 incidentes semanales.

Los ataques cibernéticos contra manufactureros se han desatado debido al impacto que un solo ataque exitoso puede generar. Paralizar una línea productiva, puede costar millones de dólares para las empresas, lo que lo vuelve conveniente para que grupos delictivos extorsionen, roben información y cometan fraudes entre otras actividades ilícitas.

El informe identifica 44 actores activos hasta marzo de 2026, con tres dominando en la escena internacional: **Akira**, un grupo activo desde el 2023 que opera mediante ataques selectivos, se estima que sus ganancias rondan los 244 millones de dólares al cierre del 2025; **Qilin**, opera desde Rusia cifrando sistemas, filtrando datos críticos y extorsionando a sobre clientes y proveedores; y **Play**, el grupo se distingue por desactivar los controles de seguridad antes de atacar, dejando a sus víctimas sin capacidad de respuesta inmediata.

Especialistas resaltan que la mayor amenaza cibernética en las empresas es la falta de conocimiento y capacitación, aunque también mencionan al reto de la regulación, ya que dependen de directrices y regulaciones locales y nacionales que pueden ser una limitante.

Consultores Internacionales Ansley *es una empresa de consultoría establecida en la Ciudad de México, enfocada a proveer asesoría estratégica a gobiernos y empresas en materia de políticas públicas, comercio internacional y asuntos regulatorios y de inversión*.