TECNOLOGÍA

La protección de datos marca la agenda de las empresas en 2024

Inteligencia artificial, biometría o consentimiento condicionado son algunos de los retos con gran impacto para empresas y administraciones que deben afrontar en los próximos meses.

Laura Saiz. Madrid

El reglamento europeo de inteligencia artificial (*AI Act*) entrará en vigor en 2026, aunque algunos de sus apartados lo hará antes, como los usos prohibidos. 2024 será un año crucial para las empresas en cuanto a su adaptación no sólo a las nuevas normas sobre IA, sino también a todas aquellas relacionadas directamente con la protección de datos.

Lo confirman desde el área de tecnología, medios y telecomunicaciones (TMT) de Ecija: "El final de 2023 nos ha dejado diferentes enseñanzas en materia de protección de datos, en muchos casos derivadas de las propias resoluciones de la autoridad de control, así como pronunciamientos de los tribunales. De todas ellas, nacen retos con un importante impacto para las propias empresas y administraciones".

Fotos: Dreamstime

Tres de cada diez prohíben el uso de la IA generativa por los riesgos de privacidad, según un informe de Cisco.

IA generativa

Nueve de cada diez organizaciones españolas consideran que la IA requiere nuevas técnicas para gestionar los datos y los riesgos, según el informe anual *Cisco Data Privacy Benchmark*, que indica que tres de cada diez prohíben el uso de la IA generativa por los riesgos de privacidad.

"La recopilación y análisis de grandes volúmenes de datos por la IA plantea importantes retos sobre la privacidad, entre los que cabe destacar el hecho de que se hayan empleado para entrenar los algoritmos datos personales sin contar con la legitimación para realizar dicho tratamiento, o los importantes riesgos de que puedan producirse fugas de información que contiene datos personales, ante las preguntas que los usuarios realizan a las inteligencias artificiales, así como el hecho de que los propios algoritmos puedan implicar sesgos inadvertidos en la toma de decisiones, afectando potencialmente la equidad y la transparencia", señala el socio de Ecija Alonso Hurtado.

Biometría

La publicación de la guía de la Agencia Española de Protección de Datos (AEPD) sobre tratamientos de datos biométricos con finalidades de control de acceso y control de presencia en diciembre de 2023 parece poner en tela de juicio, según la socia María González, la legitimación respecto del uso de este tipo de sistemas de identificación biométrica en el entorno laboral, si bien podría hacerse extensiva a otros procesos de identificación.

Consentimiento

Meta anunció en octubre que cobrará 10 euros a aquellos usuarios que quieran evitar el uso de sus datos con fines publicitarios, algo que rápidamente han implantado muchos portales web.

"Lo que antes era claramente un modelo de acceso *libre*, se está convirtiendo en un modelo de acceso vinculado a la aceptación del uso de los datos personales con finalidades de explotación publicitaria o para enriquecimiento del editor o el pago de una cantidad para evitar dicho tratamiento de datos.

Sin embargo, a expertos como el abogado Javier Arnaiz les genera muchas dudas: ¿el usuario tiene una libertad real a la hora de aceptar el uso de sus datos con el condicionante del pago de una cantidad económica? ¿Es exigible a estas plataformas que no vinculen el consentimiento al pago de una cantidad económica?

Procedimientos sancionadores

La AEPD es la autoridad más activa en cuanto a sanciones. Según el último CMS Enforcement Tracker, España había registrado 583 multas desde la aplicación del reglamento europeo de protección de datos, muy por encima de las 246 de Italia, aunque por valor es Irlanda la más destacada con más de 1.309 millones de euros en total. "La elevada actividad sancionadora de las autoridades de control continúa siendo motivo de preocupación para las empresas", afirma Joaquín Cives, que asegura que se pueden evitar aperturas de procedimientos sancionadores o, al menos, no limitar las posibilidades de defensa con un conocimiento adecuado de la forma de entender la protección de datos por parte de la autoridad de control española.

ASPECTOS DESTACADOS

Responsabilidad proactiva

El socio de Ecija Daniel López insiste en que "es necesario avanzar en sistemas de diligencia debida que posibiliten un mayor conocimiento de los terceros con los que se trabaja y su grado de cumplimiento efectivo de la normativa existente". En este sentido, las empresas deben ser especialmente diligentes con los datos no sólo en la contratación de proveedores, cuestión que ya se incluye en el RGPD, sino también durante la vida útil del contrato y, por tanto, del servicio. Estamos ante un proceso de evaluación continua, que no debe quedar en la petición de meros certificados, ya que esta diligencia afecta a la posibilidad de llevar a cabo procesos de evaluación o auditoría y, por tanto, de solicitar determinadas evidencias.

Ciberseguridad

El impacto en materia de ciberseguirdad en lo relativo al tratamiento de los datos tiene un impacto este 2024 en cinco principales focos, según alerta Jesús Yáñez, socio de Ecija. Así, destaca la transposición al ordenamiento jurídico español de la directiva CER en materia de resiliencia de entidades críticas; la transposición de la directiva NIS2 para la resiliencia de entidades esenciales e importantes; la implementación de obligaciones del reglamento DORA para entidades financieras, aseguradoras y prestadores de servicios de tecnologías de la información para estas entidades; la aprobación de 'Cyber Resilience Act' en materia de seguridad de productos con componentes electrónicos; y el desarrollo de los marcos de certificación en materia de ciberseguridad impulsados por Enisa.

Intermediarios

La plena aplicación de la la Ley de Servicios Digitales (DSA) prevista para el 17 de febrero busca, en palabras de Esperanza López, "proteger el entorno digital frente a la difusión de contenidos ilícitos, reforzando los derechos fundamentales de los destinatarios de los mismos". Entre otras, la DSA impone obligaciones a los prestadores de servicios en línea, a la vez que refuerza la protección de datos, especialmente en lo relativo a la elaboración de perfiles, es decir, en el análisis de aspectos determinados de una persona con el fin de predecir su comportamiento o intereses y, de esta manera, adoptar decisiones sobre ella. Así, la DSA impedirá mostrar anuncios basados en datos especialmente protegidos o de menores o usar 'interfaces' engañosas.