

4 DÍA INTERNACIONAL DE LA PROTECCIÓN DE DATOS PERSONALES

La expansión acelerada de la inteligencia artificial (IA) está abriendo un nuevo frente de debate en empresas y usuarios: cuánto dato es legítimo usar, para qué fines y bajo qué condiciones. En la práctica, la promesa de productividad y eficiencia convive con una creciente inquietud por la privacidad, los sesgos algorítmicos y la pérdida de control sobre información sensible.

"El principal dilema es la tensión entre la protección de datos personales y la necesidad de grandes volúmenes de información para entrenar modelos que impulsen la productividad", plantea el director ejecutivo del Centro Nacional de Inteligencia Artificial (Cenia), Rodrigo Durán.

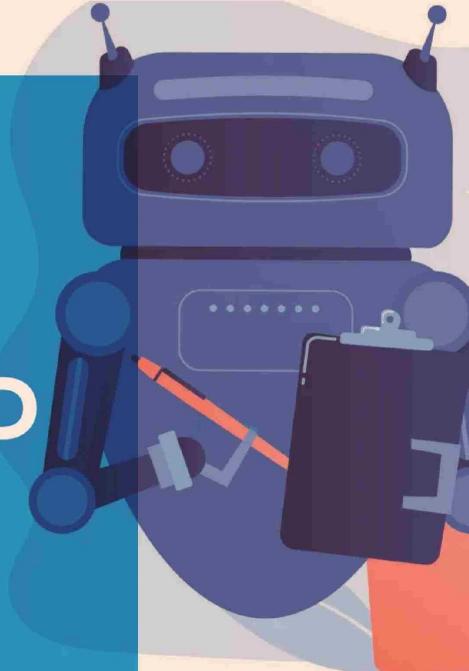
El ejecutivo añade que "en Chile, la IA generativa representa una oportunidad de aceleración equivalente al 12% del PIB, pero la regulación debe ser habilitante, no solo restrictiva".

El problema es que la capacidad real de gobernar estos sistemas todavía es baja. Según cifras del Cenia, "solo el 21% de las organizaciones asigna la gobernanza de IA a ciberseguridad o privacidad, y apenas el 14% tiene roles dedicados a gobernanza". En paralelo, agrega Durán, "los incidentes relacionados con IA han crecido drásticamente a nivel global y la confianza pública está cayendo".

EL DELICADO EQUILIBRIO ENTRE PRODUCTIVIDAD Y PRIVACIDAD EN LA ERA DE LAIA

Entre la promesa de aumentar la eficiencia en contextos empresariales y la creciente presión regulatoria, expertos advierten que el verdadero desafío no es usar más datos, sino gobernarlos sin perder la confianza.

POR ANAÍS PERSSON



Esa brecha entre ambición tecnológica y control es la que empieza a chocar con la nueva Ley de Protección de Datos Personales, cuya implementación total debe concretarse en diciembre de este año.

Dilemas asociados

Para el CEO de LeyDeDatos, Rodrigo Zigante, "existe una fricción técnica y legal evidente entre cómo



operan muchos sistemas de IA y lo que exige la norma". Uno de los puntos críticos es la explicabilidad: "El primer punto de tensión es el derecho a obtener una explicación frente a la opacidad de los modelos de 'caja negra'; garantizar explicabilidad en redes neuronales es un desafío estadístico complejo".

A eso se suma el derecho de las personas a oponerse a decisiones

automatizadas. "Habilitar intervención humana cuando el titular solicita cambiar flujos, eleva costos y afecta directamente la rentabilidad", dice Zigante.

Además, hay un tercer choque: "En una base de datos basta eliminar el registro, pero en un modelo de IA el entrenamiento transforma información en parámetros propios del modelo. Borrar el dato fuente no

necesariamente borra la influencia que tuvo en el 'conocimiento' del modelo".

El CEO de Lemontech, Lautaro Rodríguez, sostiene que "el principal dilema ético hoy no es si la IA puede automatizar procesos, sino bajo qué condiciones se utilizan los datos personales para hacerlo".

En su diagnóstico, los riesgos se mueven en dos planos. "Por un lado están los sesgos y las alucinaciones del modelo, que se gestionan con diseño responsable y supervisión humana. Pero el riesgo verdaderamente crítico es la seguridad y privacidad de los datos", afirma. "El mayor riesgo hoy no es que la IA se equivoque, sino que los datos pierdan control. Y en el mundo legal, la confianza no se negocia: se diseña, se gobierna y se protege desde el primer día", sostiene.

Según el CTO de Soyio, Matías Menich, "se trata de datos especialmente sensibles, que no pueden ser reemplazados ni rotados en caso de uso indebido". El problema, explica, es que "cuando estos datos alimentan sistemas de IA, muchas veces opacos incluso para las propias organizaciones, se vuelve complejo garantizar que se utilicen solo para el fin informado y que las decisiones automatizadas puedan ser explicadas y auditadas".

A eso se suma la reutilización para fines secundarios y la transferencia internacional de datos: "Sin una

DÍA INTERNACIONAL DE LA PROTECCIÓN DE DATOS PERSONALES 5

21%

DE LAS EMPRESAS ASIGNA LA GOBERNANZA DE IA A CIBERSEGURIDAD O PRIVACIDAD, SEGÚN EL CENIA.

14%

DE LAS EMPRESAS TIENE ROLES DEDICADOS A GOBERNANZA DE DATOS.

"El mayor riesgo no es que la IA se equivoque, sino que los datos pierdan control. Y en el mundo legal, la confianza no se negocia: se diseña, se gobierna y se protege desde el primer día", afirma el CEO de Lemontech, Lautaro Rodríguez.

gobernanza clara, las organizaciones quedan expuestas a riesgos regulatorios, reputacionales y operativos relevantes", dice.

Desde la perspectiva de los usuarios, el manejo sigue siendo limitado. "Hoy el control que tienen las personas sobre sus datos sigue siendo más formal que efectivo", dice Menich. "Existe una brecha relevante entre el consentimiento otorgado originalmente y el uso efectivo de los datos", agrega.

El ejecutivo menciona que "muchas empresas aún no cuentan con la infraestructura técnica necesaria para mapear, controlar y auditar el uso de datos personales en entornos de IA. El desafío no es solo normativo, sino de capacidades reales para gobernar estos sistemas en el día a día".

El consenso entre los expertos está en que la respuesta no pasa por frenar la innovación, sino por rediseñarla. "La ética no es un complemento de la tecnología; es parte esencial de su arquitectura", concluye Rodríguez.