

Suscríbete hoy

MILENIO + The Times

TECNOLOGÍA

OPINIÓN Última Hora M+ Política DOMINGA Estados Policía Narcotráfico Negocios Infografías Mundo Estilo Cultura Laberinto



Vigilancia, censura y datos a la venta: el mapa de las amenazas digitales en América Latina

La IA y las filtraciones de datos ponen en riesgo la privacidad en la región, según un informe que expone las consecuencias para la seguridad digital.

Angela Molina

Ciudad de México / 23.10.2026 13:31:00



| Únete al canal de Milenio

+ Agregar Milenio en

M+ Estudios médicos a la venta, plataformas bloqueadas e imágenes sexuales fabricadas con **inteligencia artificial** (IA), son algunas de las amenazas digitales en América Latina que afectan la **privacidad**, la **libertad de expresión** y la **participación política**. Detrás de ellas aparecen delincuentes, pero también gobiernos y empresas, advierte la organización **Derechos Digitales**.

El informe **En la mira 2** reúne más de 100 casos y analiza patrones regionales de vigilancia, censura, filtraciones y violencia digital. Su periodo principal de estudio comprende de **junio de 2024 a mayo de 2025**.

En entrevista con **MILENIO**, Ximena Cuzcano, analista de Seguridad y Resiliencia Digital de Derechos Digitales y una de las autoras, explica que la investigación busca

mostrar las consecuencias de estos incidentes para los derechos humanos.

El trabajo combina monitoreo semanal de fuentes abiertas con investigaciones y acompañamiento de las 14 organizaciones del Observatorio Latinoamericano de Amenazas Digitales. No es un *ranking* pues la censura, el subregistro y las diferencias para documentar casos impiden comparar directamente la seguridad de los países.

➔ Te recomendamos



Tenemos que lograrlo lo más pronto posible: Ebrard busca reducir aranceles de EU a autos, acero y aluminio



Elon Musk y Starlink adquieren una cartera de espectro de “banda baja”

Datos sensibles en el mercado ilegal

Las filtraciones fueron identificadas en 12 países (Argentina, Brasil, Chile, Colombia, Costa Rica, Ecuador, Honduras, México, Paraguay, Perú, Uruguay y Venezuela), además de incidentes de alcance regional. En Argentina se pusieron a la venta más de 665 mil estudios médicos, entre ellos radiografías, tomografías y pruebas de laboratorio. En Uruguay quedaron expuestas casi 15 mil solicitudes de visa, correspondientes principalmente a personas migrantes y refugiadas.

El reporte señala fallas básicas, como bases de datos accesibles sin autenticación, recolección excesiva de información y servicios tecnológicos contratados sin controles suficientes.

“No es que hay un *hacker* experto y esté hackeando a todos los organismos, sino son vulnerabilidades que las mismas instituciones no están parchando. Entonces, de alguna manera están estos datos en el mercado ilegal y son los ciberdelincuentes quienes cometen fraude: con un nombre, un DNI y una fecha de emisión podrían sacar un préstamo”, señala Cuzcano.

La información expuesta puede alimentar fraudes, extorsiones o vigilancia. La analista advierte una contradicción: mientras los gobiernos anuncian la adopción de IA para modernizar sus procesos, mantienen

LAS MÁS VISTAS

1



GRUPO MILENIO

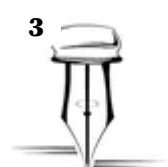
Transportistas protestan en carreteras de Guanajuato
HOY 26 de octubre | Bloqueos, cierres y actualizaciones

2



¿Qué carreteras están CERRADAS hoy 26 de octubre por Paro Nacional de Transportistas? Aquí hay manifestaciones

3



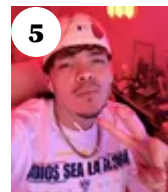
Una advertencia de Lula a México

4



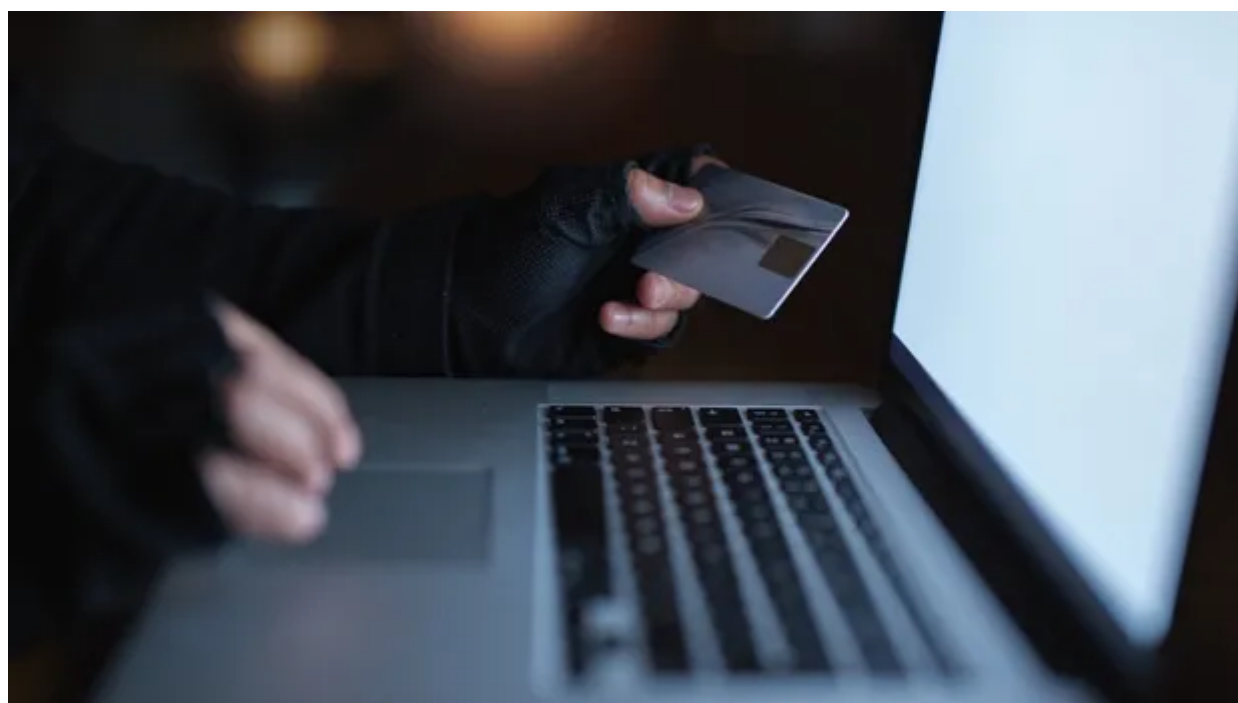
Manifestaciones HOY 26 de octubre: Calles y autopistas cerradas por BLOQUEOS viales y marchas en CdMx y Edomex | EN VIVO

5



¿Por qué Komanche recibía tanto hate? Las polémicas y acusaciones que enfrentó el streamer antes de morir

infraestructuras débiles para proteger los datos que ya recaban.



En las filtraciones fueron identificadas en 12 países, entre ellos, México. | Foto: Especial

Amenazas digitales en América Latina

Una diferencia frente a la edición anterior es la presencia de inteligencia artificial en múltiples amenazas. Se utiliza para fabricar imágenes sexuales sin consentimiento, producir desinformación electoral y ampliar capacidades de vigilancia.

En **Venezuela** circularon audios falsos atribuidos a la opositora **María Corina Machado** y elaborados con IA. En **Brasil** se documentaron al menos cinco ataques con imágenes sexuales manipuladas contra candidatas, una forma de intimidación que cruza la desinformación con la violencia de género.

Cuzcano explica que estas herramientas dificultan reconocer los engaños ya que pueden generar textos convincentes e imágenes que imitan elementos de fuentes oficiales.

“Antes, si te das cuenta que está mal escrito, probablemente sea una *fake news*, pero ahora con la IA tú le puedes decir al chatbot que genere un texto súper bueno y lo va a hacer, igualmente a nivel de imágenes, vimos que había noticias que replicaban logos institucionales, entonces como que se veía más real”.

El informe también retoma un estudio que identificó 105 aplicaciones de *deepfake* disponibles en **Google Play** a diciembre de 2024; **89.5 por ciento** representaban un peligro potencial para las mujeres. Estas herramientas permiten manipular rostros e imágenes y pueden facilitar

agresiones sexuales digitales.

Para la investigadora, las **plataformas** tienen responsabilidad por permitir la distribución de esas aplicaciones y por sus mecanismos insuficientes de supervisión. Entre los efectos de la **violencia** advierte el retiro de **mujeres** de espacios de expresión y participación.

“Como **mujeres** estamos expuestas lamentablemente a mucha violencia [...] Entonces se está normalizando el censurarse para escapar de ese tipo de violencia”.



El reporte señala fallas básicas, como bases de datos accesibles sin autenticación. | Foto: Especial

Seguridad como argumento para vigilar

El estudio identifica una expansión de las facultades estatales de monitoreo, frecuentemente justificada por la seguridad nacional o el orden público, sin controles equivalentes de transparencia y rendición de cuentas.

En **Venezuela**, tras las elecciones de **2024**, se bloquearon plataformas como Signal, X, **TikTok** y **Telegram**. También se restringieron sitios de proveedores de **VPN**, herramientas utilizadas para intentar eludir la censura. En **Nicaragua** fueron bloqueados dominios de medios independientes.

La investigación aborda además la captación de datos biométricos mediante **World**, antes **Worldcoin**, que ofrecía incentivos económicos por escanear el iris. Cuestiona las condiciones del consentimiento en contextos de precariedad: a diferencia de una contraseña, el iris o el rostro no pueden sustituirse si quedan comprometidos.

Para **Cuzcano**, otro riesgo es asumir las filtraciones como inevitables y conformarse con respuestas tardías de las

entidades responsables. Esa resignación, advierte, puede reducir la exigencia de protección mientras la información continúa circulando.

“Otra cosa que se está normalizando mucho son las filtraciones de datos. He escuchado a muchas personas que dicen ‘mis datos se filtraron, bueno’ y aceptan esos comunicados tardíos que sacan las empresas y entidades estatales, que es lo único que he visto en términos de reacción, diciendo que van a aplicar sus medidas, otros diciendo que no, que es mentira”.

La investigación, disponible: [aquí](#), advierte que las capacidades de vigilancia y control avanzan más rápido que los mecanismos para exigir transparencia y proteger a las personas. Las consecuencias también alcanzan la vida fuera de internet: inhiben la participación política, debilitan redes de apoyo y limitan la libertad de expresión. Frenarlas exige que gobiernos y empresas rindan cuentas por las tecnologías que utilizan y por los datos que tienen bajo su resguardo.



Gobierno mantienen infraestructuras débiles para proteger los datos que ya recaban, afirma. | Foto: Especial

MRA

Síguenos en [Google News](#)

➔ TAGS RELACIONADOS:

Inteligencia Artificial

Ciberseguridad

Datos Personales



Queda prohibida la reproducción total o parcial del contenido de esta página, mismo que es propiedad de MILENIO DIARIO, S.A. DE C.V.; su reproducción no autorizada constituye una infracción y un delito de conformidad con las leyes aplicables.

 **INICIA LA CONVERSACIÓN**