Filtraciones de datos crecen en el país sin controles ni consecuencias claras

Al menos 11 ataques informáticos han afectado a empresas privadas y entes públicos en el país desde 2024, exponiendo datos personales de usuarios, contribuyentes y clientes. Es un tema del que poco se habla o que va quedando en el olvido en medio de un país donde, aunque existen normas sobre privacidad, no hay un sistema efectivo que garantice la protección de los datos personales ni obligue a rendir cuentas.

Los casos verificados por la ONG Redes Ayuda incluyen ataques a empresas de telecomunicaciones como Digitel, Movistar y Fibex Telecom; instituciones financieras como el Banco Nacional de Crédito (BNC); plataformas digitales como Cashea, Yummy Rides y Rapikom; y organismos públicos como el Seniat, el Metro de Caracas, Conviasa y hasta Pdvsa. Algunos de estos episodios implicaron filtración de datos, intrusiones en sistemas o ataques de ransomware.

Pero la cifra de filtraciones o hackeos podría ser aún mayor, pues han circulado reportes sobre posibles vulneraciones en cuerpos de seguridad como el Cuerpo de Investigaciones Científicas, Penales y Criminalísticas (Cicpc), el Servicio Bolivariano de Inteligencia Nacional (Sebin), Polichacao y otras instituciones. Sin embargo, en estos casos no ha habido confirmación oficial ni tampoco desmentidos, lo que evidencia la falta de transparencia en torno a estos incidentes.

Aunque los términos hackeo y filtración de datos suelen usarse como sinónimos, no todo hackeo implica necesariamente la exposición de información. Luis Serrano, coordinador general de Redes Ayuda, explica que en el contexto actual ambos fenómenos están estrechamente vinculados: «Lo que está ocurriendo ahora es que esa filtración de datos es consecuencia de hackeos».

Para Serrano, el aumento de estos incidentes no es casual y responde a una combinación de factores: baja protección, mayor exposición digital y un entorno donde la información puede convertirse en mercancía.
Añade que el hecho de que al país vaya a ingresar más dinero «llama la atención de muchos atacantes». Por otra parte, expone que la inversión en ciberseguridad «es dejada de lado; se invierte lo mínimo, o tienen sus sistemas abiertos».

«A partir del 3 de enero, con la captura de Nicolás Maduro, varios atacantes se dieron cuenta de que en Venezuela había una data valiosa que se podía vender, hackear, una economía más o menos funcionando y poca inversión en materia de seguridad», especifica el también defensor de derechos digitales y derechos humanos.

Datos, negocios y vulneraciones

Las bases de datos con información personal pueden circular casi de forma gratuita o comercializarse en foros clandestinos o canales privados por cientos o miles de dólares. Esta información permite perfilar a los ciudadanos con precisión.

Luis Serrano lo explica con un ejemplo: si alguien accede a los datos de una empresa puede identificar hábitos de consumo, ubicación o patrones de uso de un usuario y utilizar esa información para ejecutar «un phishing teledirigido, hackear su WhatsApp y afectar a su círculo inmediato, sacarle dinero o información».

Tanto las empresas como los entes públicos tienen la obligación de resguardar la privacidad de sus usuarios y, aunque Serrano admite que «es difícil hablar de temas de derechos humanos (con la filtración de datos)» en estos casos, reconoce que «sí hay una vulneración a la privacidad de las personas».

La exposición de datos también puede tener implicaciones políticas. El representante de Redes Ayuda lo ilustra con una práctica frecuente en el país: «Cuando a ti te llega un mensajito de Nicolás Maduro Guerra, hubo una vulneración de los datos», afirma, en referencia al uso de información personal para envíos masivos con fines políticos.

Casos similares han sido asociados a otros actores públicos, lo que abre interrogantes sobre el acceso, manejo y uso de la información personal en Venezuela.

El abogado Ángel Díaz, especialista en ciencia y privacidad de datos, sostiene que «el Estado es el principal filtrador de datos de Venezuela», por medio de entes como el Consejo Nacional Electoral (CNE), el Tribunal Supremo de Justicia y otras instituciones en las que con introducir el número de cédula se obtiene información de cualquier persona; lo que advierte agrava los riesgos de los ciudadanos.

La exposición de datos personales puede traducirse en impactos concretos en la vida cotidiana: fraudes, suplantación de

identidad, acceso a cuentas y extorsión. Pero también plantea dudas sobre cómo se recolectan, almacenan y utilizan los datos en un contexto con escasos controles.

Existen normas, pero sin sanciones

A diferencia de lo que suele afirmarse, en Venezuela sí existen normas que abordan la protección de datos personales, aunque de forma fragmentada.

Ángel Díaz, también defensor de los derechos digitales, explica que en el país «sí hay leyes que regulen la materia, especialmente en los temas de protección de datos». Detalla que hay una sentencia vinculante del Tribunal Supremo de Justicia y no «una ley específica».

> *«Existe una ley regulatoria, poco conocida y aplicada por nadie», resume el especialista.*

Asimismo, el abogado advierte en el tema de sanciones, con respecto a la filtración de datos, que existe «una zona gris», pues afirma que «no hay sanciones»; por lo que no se puede castigar al responsable del manejo de estos.

> *Estas debilidades impactan directamente en los ciudadanos. La legislación vigente considera como «víctima a la empresa o institución que sufre el ataque y no a las personas cuyos datos fueron expuestos», precisa Díaz.*

Esto limita las posibilidades de reclamo y deja a los afectados sin mecanismos reales de reparación, especialmente cuando proviene de organismos del Estado.

Opacidad y control de daños

La falta de regulación también influye en cómo las organizaciones responden a estos incidentes. En varios casos recientes de filtración de datos, las empresas han optado por minimizar lo ocurrido o limitar la información pública. En lugar de alertar a los usuarios sobre posibles riesgos, los comunicados se enfocan en proteger la reputación corporativa.

«Buscan más controlar el daño reputacional que proteger a los usuarios ante la exposición de sus datos», señala Luis Serrano.

Sin información clara, los usuarios desconocen los riesgos y no toman medidas preventivas frente a posibles fraudes.

Para el coordinador de Redes Ayuda, la solución a la filtración de datos pasa por dos vías: la creación de una ley que proteja a los ciudadanos y una mayor exigencia en los protocolos de seguridad de entidades públicas y privadas. «Tiene que haber una mayor exigencia de lo robustos que deben ser esos sistemas», advierte.

Por su parte, el abogado especialista en privacidad de datos Ángel Díaz considera necesaria una ley específica, similar al Reglamento General de Protección de Datos de la Unión Europea, que establezca responsabilidades, límites y mecanismos de control efectivos. Pero insiste en que el problema va más allá de la legislación.

Díaz sostiene que también es urgente crear una autoridad especializada que supervise el manejo de la información y reformar prácticas institucionales arraigadas. «En Venezuela el Estado sospecha del ciudadano y por eso le exige más datos de los necesarios», explica.

A su juicio, la protección de datos no se limita a evitar estafas: también implica impedir el uso indiscriminado de la información por parte de empresas y del propio Estado, con fines comerciales, políticos o de control: «Se trata de un cambio completo en la forma en que se conciben los datos y el rol del ciudadano», afirma. Sin ese cambio estructural —legal, institucional y cultural—, considera, la exposición de datos seguirá creciendo y sus consecuencias serán cada vez más profundas.

Con información de TalCual