EXPLICATIVOS

En Latinoamérica se venden datos personales a través de Telegram: Conoce más sobre estos delitos

Por **Esteban Cárdenas** Marzo 13, 2026

La compraventa ilegal de datos personales en Telegram no es un problema marginal ni solo técnico. La investigación *Identidades en venta*, realizada por 'Derechos Digitales', documenta un mercado activo y regional en el que identidades, direcciones, historiales financieros, datos de salud, vínculos familiares y hasta documentos oficiales circulan como mercancía. El estudio identificó 27 grupos y canales activos en Brasil, Perú y Argentina, operados con bots, pagos digitales y una lógica comercial estable, lo que muestra que la identidad de las personas ya funciona como un insumo económico dentro de una economía clandestina digital.

Lo más relevante para entender el contexto regional es que este mercado combina varios rasgos típicos de la criminalidad organizada: infraestructura persistente, automatización, división de roles, monetización constante, operación transfronteriza y aprovechamiento de debilidades estatales. La investigación no concluye que todo el material provenga del Estado, pero sí advierte indicios consistentes de que parte de la información podría venir de bases públicas o registros oficiales, por coincidencias de formato, terminología, estructuras técnicas y marcas institucionales.

¿Cómo funciona este mercado?

Telegram aparece en el informe como una plataforma especialmente útil para este comercio por varias razones: permite grupos de hasta 200.000 miembros, archivos grandes, canales de difusión masiva, interacción mediante bots y un grado de anonimato superficial porque no obliga a exponer el número telefónico públicamente. Aunque fue presentada como una plataforma centrada en privacidad, el informe recuerda que no cifra de extremo a extremo por defecto y que almacena metadatos y otros datos de usuarios en la nube.

La metodología de la investigación se desarrolló entre octubre de 2024 y noviembre de 2025, con tres fases: exploración, observación y análisis. Se usaron búsquedas manuales y automatizadas, técnica de "bola de nieve", monitoreo de denuncias en redes y observación no participante. Los investigadores no contactaron a administradores ni compradores y evitaron reproducir daño publicando nombres o enlaces de los grupos.

El mercado no opera de una sola manera. En Brasil predominó un modelo altamente automatizado, con bots administradores, consultas gratuitas limitadas y cobro por acceso ampliado. Los planes iban desde 1 dólar por una semana hasta 78,80 dólares por dos años, y el pago se hacía por PIX. En Perú también predominó el freemium, con resultados parcialmente ocultos para empujar la compra; allí los precios fueron desde 2,20 dólares por tres días hasta 116,20 dólares anuales, con pagos vía Yape y Plin. En Argentina, en cambio, el sistema fue más personalizado: los canales servían como vitrina, pero la venta se cerraba por chat privado, con vendedores humanos, tokens o accesos temporales y pagos por Mercado Pago o criptomonedas.

¿Qué tipo de datos se venden?

Los hallazgos muestran niveles de exposición extraordinariamente altos. En Brasil, el comando **/cpf** devolvía no solo identificación básica, sino renta estimada, clasificación socioeconómica, scoring crediticio, historial laboral, PIS, acceso a programas sociales, líneas telefónicas, domicilios múltiples, red familiar, vecinos e incluso historial de vacunación, con campos que parecían extraídos de bases de datos estructuradas.

En Perú, el comando **/dni** permitía acceder a nombres, sexo, fecha y lugar de nacimiento, estado civil, grado de instrucción, estatura, fechas de emisión y caducidad, donación de órganos, nombres y DNI de padre y madre, domicilio, huellas dactilares, foto, firma y hasta imágenes completas del DNI físico, electrónico o virtual, incluso de niñas, niños y adolescentes. También aparecían comandos para datos de hogar, clasificación socioeconómica, líneas celulares y certificados aparentemente oficiales de antecedentes policiales y judiciales.

En Argentina, el comando **/dni** ofrecía imagen facial, firma, CUIL, número de trámite, emisión y vencimiento del documento, nacionalidad, sexo, fecha de nacimiento, dirección completa e incluso enlaces a Google Maps. Otros comandos permitían información financiera, familiar, laboral, telefónica y de empresas. El informe destaca, además, la presencia de elementos técnicos como MRZ (bloque de texto con caracteres alfanuméricos y símbolos situado en el DNI para una lectura automática del documento), códigos de barras, que sugieren acceso a capas profundas del sistema de identidad.

¿Por qué esto importa para entender el crimen organizado?

La investigación no usa el término "crimen organizado" como etiqueta penal cerrada, pero sí describe un ecosistema con rasgos compatibles con operaciones criminales estructuradas. Hay automatización 24/7, jerarquías entre "dueño", "soporte", "admin" o "moderador", monetización sostenida, marketing digital, esquemas de fidelización, operación regional y uso de pasarelas de pago o criptoactivos. No parece una suma de filtraciones aisladas, sino una economía ilícita estable que convierte la información personal en mercancía.

Además, el fenómeno rebasa a los tres países analizados: durante el trabajo de campo se detectó circulación de datos de Venezuela, Bolivia, República Dominicana, Chile y Uruguay. Eso refuerza el carácter transfronterizo del

problema y vuelve insuficiente una respuesta puramente nacional.

Debilidades estatales y posibles orígenes públicos

Uno de los ejes más delicados del informe es la advertencia sobre posibles orígenes públicos de parte de los datos. No hay una atribución concluyente, pero sí señales técnicas relevantes: estructuras JSON, nomenclaturas tipo campo:valor, uso de camelCase, campos “null”, marcas institucionales, tiempos de emisión coincidentes con las consultas y referencias explícitas a scraping o credenciales.

A partir de eso, la investigación identifica tres fragilidades estructurales en América Latina. La primera es **normativa**: hay leyes de protección de datos y ciberdelitos, pero persisten vacíos, sobre todo para el sector público. La segunda es **institucional**: las autoridades suelen carecer de autonomía, presupuesto o capacidad para supervisar incluso al propio Estado. La tercera es **de seguridad de la información**: muchas instituciones públicas administran grandes bases de datos sin políticas robustas, auditorías regulares ni una cultura sólida de protección.

Violencia de género e infancias: el daño no es abstracto

El informe insiste en que los riesgos no son meramente técnicos. Documenta denuncias de mujeres y personas LGBTQIA+ cuyos datos fueron usados para extorsión sexual, amenazas, doxxeo (revelar intencional y públicamente información personal sobre un individuo u organización) y acoso. En Brasil, una mujer denunció amenazas tras la compra de datos suyos y de su madre; en Argentina, se compartió la foto del DNI de una mujer con comentarios misóginos y homofóbicos; en Perú, una joven recibió amenazas con armas y contra su familia junto con la filtración de su documento. El informe concluye que la disponibilidad de datos personales potencia la violencia de género facilitada por tecnologías.

También subraya la vulnerabilidad de niñas, niños y adolescentes. No solo por la venta de sus datos o documentos, sino por la estética de captación observada en algunos grupos: ilustraciones anime de niñas escolarizadas e hipersexualizadas usadas como gancho visual. El informe interpreta esto como parte de una normalización cultural de prácticas ilícitas y lo conecta con un contexto regional de violencia sexual contra infancias.

¿Qué deberían hacer los Estados y las plataformas?

Las recomendaciones del informe se ordenan en siete frentes: atención y reparación a víctimas; enfoque de género; protección de infancias; autonomía institucional; gobernanza de datos públicos; gobernanza de plataformas; y cooperación regional. Entre las medidas más concretas están: equipos conjuntos de investigación, patrocinio jurídico gratuito, apoyo psicosocial, notificación proactiva a afectados, rutas rápidas de remoción, fortalecimiento de autoridades de datos y ciberseguridad, auditorías externas a bases públicas, controles estrictos de acceso, monitoreo de consultas masivas, cifrado, transparencia sobre incidentes y cooperación regional basada en derechos humanos.

Para plataformas como Telegram, el documento plantea reportes periódicos, mecanismos de denuncia accesibles, verificación reforzada de bots y desarrolladores, respuesta rápida a órdenes judiciales y coordinación con pasarelas de pago y servicios financieros, sin caer en vigilancia indiscriminada.

Preguntas frecuentes

¿El informe prueba que los datos salieron de bases estatales?
No de forma concluyente. Lo que documenta son indicios consistentes —formatos, marcas, estructuras y

tiempos de respuesta— que justifican investigar seriamente posibles filtraciones, scraping o uso indebido de credenciales oficiales.

¿Esto ocurre solo en Brasil, Perú y Argentina?
No. Esos son los países analizados en detalle, pero durante el trabajo de campo también apareció información de otros países latinoamericanos, lo que sugiere un fenómeno regional más amplio.

¿Qué vuelve a Telegram especialmente útil para este mercado?
Su escala, los grupos y canales masivos, el uso de bots, el envío de archivos grandes, la baja moderación observada y un anonimato operativo suficiente para vendedores y compradores.

¿El principal daño es el fraude económico?
No solamente. El informe documenta extorsión, acoso, doxxeo, amenazas, violencia de género, afectaciones a infancias, revictimización y erosión de la confianza en la digitalización estatal.

¿La respuesta debe ser solo penal?
No. El informe sostiene que la vía penal es insuficiente y que se necesitan prevención, reparación, supervisión independiente, protección a víctimas y mejoras estructurales en la gobernanza de datos y plataformas.

Conclusión

La investigación retrata algo más profundo que una serie de filtraciones: muestra una infraestructura ilícita regional que monetiza la identidad y explota debilidades estatales, desigualdades sociales y vacíos de gobernanza digital. En ese contexto, el crimen organizado ya no solo trafica drogas, armas o personas; también trafica datos, perfiles, documentos y relaciones familiares. El impacto ciudadano es directo: más riesgo de fraude, extorsión, persecución, violencia de género y exposición de infancias, además de una pérdida de confianza en el Estado y en la vida digital. El hallazgo central es que América Latina no enfrenta solo un problema de ciberseguridad, sino una crisis de gobernanza de datos con consecuencias democráticas y de derechos humanos.

Bibliografía y enlaces

- Derechos Digitales. *Identidades en venta: el mercado ilegal de compra y venta de datos personales latinoamericanos en Telegram*. Investigación realizada entre octubre de 2024 y noviembre de 2025.