futurIA

Crece en el país la compra y venta ilegal de datos personales en Telegram

La información sensible de personas se ofrece en canales de Telegram; una investigación de la ONG Derechos Digitales detectó 27 espacios activos en Brasil, Perú y Argentina dedicados a su comercialización

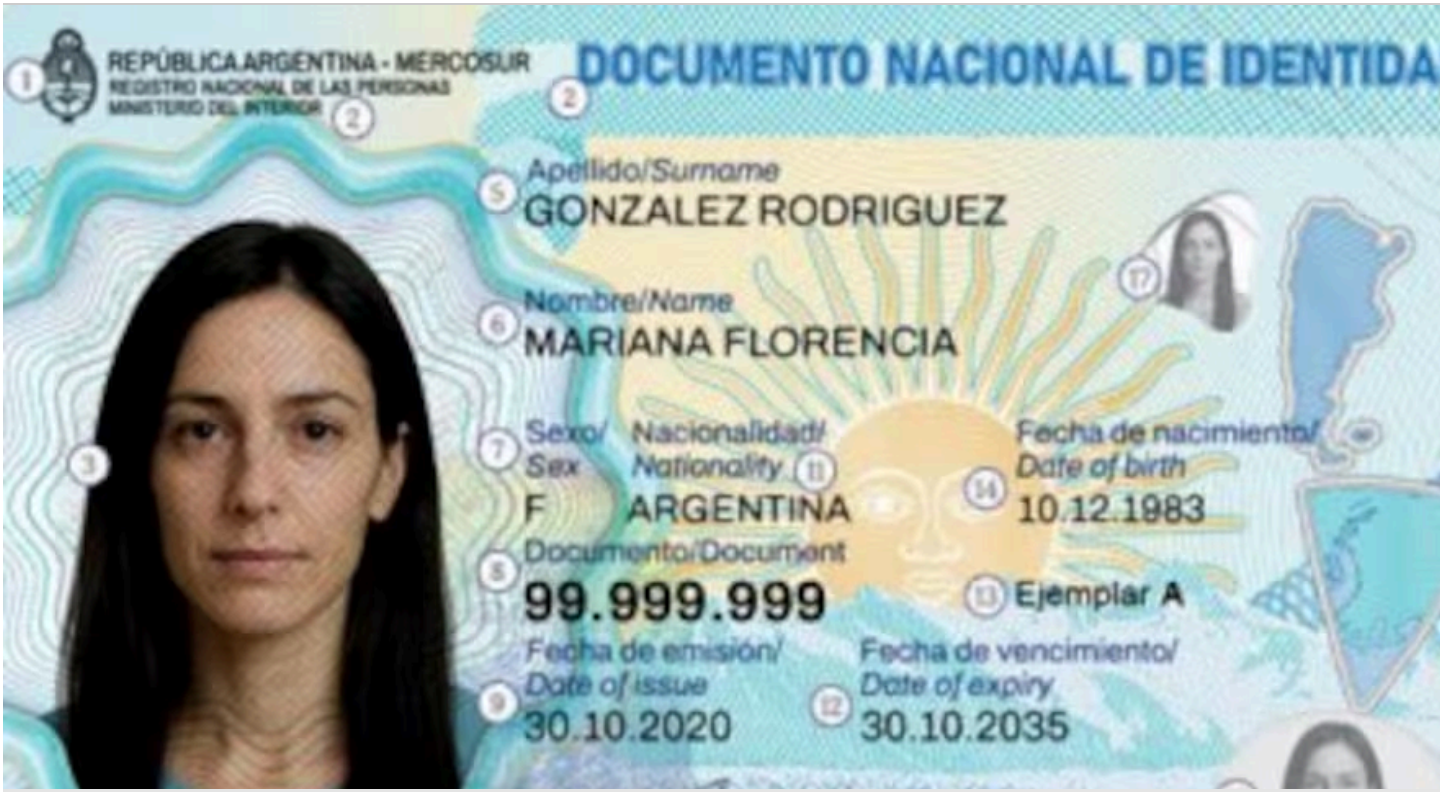
1 de abril de 2026 • 15:53

7 '

Julieta Schulkin

PARA LA NACION

ESCUCHAR NOTA



Anverso del nuevo DNI

Seguir en

La **información sensible de personas proveniente de filtraciones, técnicas de scraping y hackeos se vende en internet** y es cada vez más fácil de encontrar. Lejos de la dark web, está disponible en canales de Telegram que permiten comprar y vender ilegalmente datos personales. Una nueva investigación de la ONG Derechos Digitales detectó **27 espacios activos en Brasil, Perú y Argentina** dedicados a su comercialización.

La compra se hace en cuestión de segundos. En algunos casos, tal como detectan

violencia de género.

El estudio *Identidades en venta. El mercado ilegal de compra y venta de datos personales latinoamericanos en Telegram* analizó grupos y canales de Telegram entre octubre de 2024 y febrero de 2025. Si bien el denominador común es que estos mercados ilegales usan bots automatizados y sistemas de pago digitales, Argentina se distingue por el "contacto humano". Tiene un modelo de operación distinto al observado en Brasil y Perú. El esquema prioriza la comunicación directa y discreta entre vendedores y compradores.

Desde la ONG observan que los canales funcionan como un punto de entrada en donde **se difunden anuncios, "planes de suscripción" y evidencias de venta**. Pero las transacciones se concretan de manera personalizada a través de chats uno a uno. No son bots, sino vendedores humanos. Para comprar y vender ilegalmente datos personales, en principio, el vendedor remite los precios y medios de pago disponibles, y una vez que se realiza la transacción, se añade y activa el bot en ese chat privado.

“En Argentina predominan los canales. **En un canal no se pueden ver ni los administradores, ni los miembros, ni los bots, a diferencia de los grupos**. Por ende, las personas que administran los canales son menos rastreables. En los canales los vendedores publican capturas de pantalla con evidencia de las ventas de datos. La persona interesada escribe a uno de los administradores o moderadores en un chat privado para hacer el pago. Una vez hecho el pago, se activa un bot con el cual la persona que compró el acceso empieza a realizar consultas sobre los datos. En varios canales se utilizan criptomonedas como forma de pago, lo que dificulta la trazabilidad de los mismos. No obstante, también se utiliza Mercado Pago, lo que sí permitiría tener cierta trazabilidad”, señala Rafael Bonifaz, líder del Programa Latinoamericano para la Resiliencia y Defensa Digital (LAREDD) de Derechos Digitales.

Cuánto valen tus datos

En Argentina, los vendedores ilegales de datos personales suelen ofrecer **distintos “planes” según el tipo y volumen de información requerida**. Por ejemplo, la investigación muestra que en algunos casos, el modelo incluye accesos temporales, es decir, permisos de uso limitado en un período determinado (por horas o días). En ese plazo, el comprador puede realizar consultas y, en ciertos casos, descargar los resultados. En otros casos, se comercializan p**aquetes por volumen de búsquedas,** que restringen la cantidad de datos obtenidos en función del valor del pago realizado.

La investigación identificó paquetes que **ofrecen acceso desde 3,5 dólares por día** (con uso del bot habilitado solo por 24 horas) hasta **servicios "permanentes" por 15 dólares, que dan acceso sin límites**. También se encontraron modalidades basadas en tokens, como la venta de 1000 unidades de datos por 100 dólares (cada token equivale a una consulta o una función habilitada dentro del bot).

¿Qué datos venden?

"En el caso de Argentina, venden **datos relacionados a DNI, CUIL, domicilio**, en ocasiones con enlace de Google Maps. Además, se tiene **información financiera y laboral como informes de Nosis** -una de las plataformas más conocidas en Argentina para reportes financieros y de riesgo crediticio- con datos financieros que incluyen **scoring crediticio, deudas**, etc. También se encuentran **datos de vínculos familiares** (padres, madres, hijos e hijas) y sus respectivos datos personales", detalla Bonifaz.

Los bots que operan en los mercados ilegales en canales de Telegram devuelven resultados que incluyen datos que habrían sido obtenidos del Registro Nacional de las Personas. Aunque también en la investigación encontraron un caso alarmante en donde se exponía la imagen de una adolescente, junto a datos como nombre, DNI y fecha de nacimiento, con una marca de agua que indicaba "**Sistema Federal de Comunicaciones Policiales**" (SIFCOP). Este sistema es una herramienta oficial restringida, usada exclusivamente para el intercambio de información de interés criminal entre fuerzas policiales y organismos judiciales. Su acceso, explican desde la ONG, está regulado por protocolos estrictos.

En algunos casos, el uso del mismo comando de consulta en el canal de Telegram puede devolver información aún más sensible y detallada, incluyendo **vínculos familiares de niñas, niños y adolescentes, como las hijas e hijos de la persona buscada**. También se identificó que el bot es capaz de devolver **tanto los datos de la persona consultada como los de sus familiares directos**.

Otros comandos de búsqueda observados incluyen el **nombre, teléfono y patente de un vehículo**. La información proporcionada incluye **datos personales, dirección completa, contactos telefónicos con nombre de la operadora, correos electrónicos, vínculos familiares (con nombres, edades y parentesco) e incluso historial laboral**, con el nombre de la empresa, estado del vínculo laboral y CUIT del empleador. Finalmente, en Argentina, también se documentó la venta de información vinculada a personas jurídicas: con el número de CUIT, los bots devuelven datos detallados sobre una entidad registrada oficialmente en el país.

De dónde vienen los datos

Uno de los hallazgos más sensibles de la investigación es el posible origen de los datos. Si bien no puede establecerse con certeza, existen indicios de que **parte de la información provendría de bases estatales o registros oficiales**. La presencia de formatos, estructuras técnicas y marcas institucionales (como códigos asociados al DNI) sugiere **vulnerabilidades en sistemas públicos como el Renaper**.

En **2021, más de 116.000 fotos del Renaper fueron filtradas y difundidas en Telegram**, y ese mismo año vulneraron la base de datos de licencias de conducir, afectando a más de seis millones de personas.

“Estamos hablando de venta de datos que podrían provenir del Renaper, del sistema financiero e incluso de sistemas policiales que, en teoría, cuentan con múltiples controles. Eso evidencia **una falla, no solo en la privacidad, sino sobre todo en la seguridad del Estado**. El problema no es únicamente que alguien hackea desde afuera. Hay indicios de una debilidad estructural en cómo se están protegiendo los datos personales”, explica Agustina Ordoñez, politóloga, coordinadora del Foro de Gobernanza de Internet en Argentina y asesora en la Cámara de Diputados.

“Por eso, el debate no debería centrarse solo en la ley, sino en quién es responsable cuando esa protección falla -reflexiona-. Si bien las plataformas tienen responsabilidad, el problema va más allá. La pregunta de fondo es: ¿qué está haciendo el Estado y por qué está ocurriendo esto? Argentina no tiene una ley de protección de datos actualizada. Pero incluso si la tuviera, ¿cambiaría algo? El punto crítico es la aplicación: ¿se puede hacer cumplir? ¿Por qué se están filtrando los datos? ¿Quién lo permite? Y también: ¿por qué las plataformas, sabiendo que esto sucede, no actúan de manera más contundente?”.

Por **Julieta Schulkin**

FuturIA • Privacidad • Seguridad informática