IDENTIDADES **EN VENTA**

El mercado ilegal de compra y venta de datos personales latinoamericanos en Telegram

Derechos Digitales
AMÉRICA LATINA

Derechos Digitales
AMÉRICA LATINA

Diseño por:
Cooperativa El Maizal

Esta es una publicación de Derechos Digitales, una organización independiente sin fines de lucro, fundada en 2005, que tiene como misión la defensa, promoción y desarrollo de los derechos humanos en entornos digitales en América Latina. El trabajo de investigación que da origen a esta publicación se llevó a cabo entre octubre de 2024 y noviembre de 2025.

ÍNDICE

SUMARIO EJECUTIVO

Este informe documenta la existencia y funcionamiento del mercado ilegal de compra y venta de datos personales en América Latina a través de la plataforma Telegram. A partir de una investigación empírica realizada entre octubre de 2024 y febrero de 2025 en Brasil, Perú y Argentina, se identificaron veintisiete grupos y canales activos dedicados a la comercialización de información personal. Los hallazgos muestran un ecosistema altamente automatizado, operado mediante *bots* y esquemas de pago digitales, que permite acceder de forma inmediata a datos personales –incluso sensibles– como identificaciones, direcciones, historiales financieros, laborales, de salud o familiares, convirtiendo la identidad de las personas en un insumo de valor económico.

Los indicios observados sugieren que parte de la información en circulación podría provenir, directa o indirectamente, de bases de datos públicas o registros oficiales. Si bien no es posible establecerlo con certeza, la coincidencia en formatos, terminología y estructuras técnicas, junto con la presencia de marcas institucionales, apunta a posibles vulnerabilidades en la gestión estatal de información. Este fenómeno se desarrolla en un contexto regional de digitalización acelerada de servicios públicos sin mecanismos equivalentes de seguridad, auditoría ni transparencia, lo que amplía las superficies de exposición y los riesgos de usos secundarios –incluso imprevistos– de los datos.

Los hallazgos de la investigación revelan tres dimensiones que dan cuenta de una fragilidad estructural característica de América Latina y que requiere de mayor investigación para establecer sus orígenes, causas y remedios. La primera es normativa: aunque los tres países cuentan con leyes de protección de datos, estrategias de ciberseguridad y marcos penales sobre delitos informáticos, persisten vacíos significativos, especialmente en el tratamiento de datos por parte del sector público. La segunda es institucional: las autoridades encargadas de aplicar estas normas carecen, en general, de independencia, recursos y capacidades para supervisar al propio Estado. La tercera se vincula con la seguridad de la información: los organismos públicos responsables de administrar grandes volúmenes de información carecen de políticas robustas de seguridad lo que, sumado a un historial elevado y de público conocimiento de filtraciones, refleja la ausencia de una cultura sólida de protección de la información en la región que requiere de mayor profundización.

Los riesgos derivados de este mercado ilegal no son meramente técnicos. La disponibilidad y circulación de datos personales en Telegram ha potenciado formas de violencia, incluyendo la violencia de género facilitada por tecnologías y la exposición de niñas, niños y adolescentes (NNA) a nuevas formas de vulneración. Se identificaron casos concretos en los tres países donde datos personales adquiridos o difundidos

en Telegram fueron utilizados para extorsionar, acosar o amenazar a mujeres, así como evidencias de venta y uso de información que afecta directamente a NNA y a sus familias. Estos hechos muestran cómo la explotación de datos se cruza con estructuras de desigualdad y poder preexistentes, convirtiéndose en un mecanismo de control, silenciamiento y revictimización.

En conjunto, los hallazgos evidencian que la región enfrenta un déficit estructural para traducir los marcos normativos existentes en garantías efectivas de protección. Superar esta brecha exige fortalecer la gobernanza y seguridad de los datos públicos, dotar de autonomía y recursos a las autoridades competentes, e integrar enfoques de género y de niñez en las políticas de ciberseguridad y protección de datos. La dimensión transnacional del fenómeno demanda, además, cooperación regional, mecanismos de rendición de cuentas y una acción decidida de las plataformas tecnológicas. En respuesta, este informe ofrece un conjunto de recomendaciones concretas orientadas a fortalecer las capacidades institucionales, garantizar la reparación a las víctimas y promover una digitalización estatal anclada en derechos humanos.

VOLVER AL ÍNDICE

1 INTRODUCCIÓN

La venta de datos personales se ha convertido en un negocio lucrativo dentro de la economía digital clandestina. Documentos de identidad, direcciones, números telefónicos, información bancaria e incluso registros médicos circulan sin consentimiento, exponiendo a millones de personas a distintos tipos de riesgos.

Inicialmente, este comercio ilícito se concentraba en foros clandestinos de la web oscura (*dark web*, en inglés), donde agentes maliciosos compraban y vendían bases de datos filtradas tanto de gobiernos como de empresas privadas. Sin embargo, en los últimos años, esta actividad se ha trasladado a espacios digitales más accesibles, entre ellos Telegram, una plataforma que ofrece a los vendedores mayores facilidades para conectarse con compradores sin necesidad de conocimientos avanzados.

La exposición de datos personales constituye una seria amenaza para la seguridad de las personas y el ejercicio de sus derechos fundamentales. La suplantación de identidades, la vulneración de cuentas bancarias, fraudes, extorsiones y amenazas digitales forman parte de los posibles impactos que enfrentan las personas quienes ven comprometida su información. Estas experiencias pueden generar impactos emocionales, financieros y de desconfianza hacia los entornos digitales y la participación en estos.

En América Latina, la situación se agrava debido a condiciones estructurales preexistentes. Factores como la debilidad institucional, las deficiencias en la gestión de datos y las brechas tecnológicas configuran un entorno fértil para la explotación digital. A ello se suma la ausencia de una cultura sólida de protección de datos y ciberseguridad y el desarrollo relativamente reciente y desigual de las legislaciones en la materia, lo que limita las capacidades de prevención y reparación frente a los abusos.

Estas condiciones se entrelazan con desigualdades históricas –socioeconómicas, de género, étnicas o territoriales– que hacen que los impactos recaigan de forma desproporcionada sobre poblaciones en situación histórica de vulnerabilidad. De este modo, el tráfico de datos no solo constituye una amenaza técnica, sino también una forma contemporánea de violencia que profundiza desigualdades históricas.

Este informe busca evidenciar la existencia y funcionamiento del mercado de comercialización ilegal de datos personales en América Latina a través de la infraestructura de Telegram. Con base en una investigación empírica sustentada en la observación no participante de grupos y canales dentro de la plataforma, se identificaron patrones, modalidades de operación, precios y tipos de datos, lo que permite trazar un mapa de esta economía ilegal digital.

Además de documentar este fenómeno, el objetivo principal es generar conciencia crítica de su impacto y demandar respuestas urgentes, así como mecanismos de reparación. La falta de regulación efectiva, la debilidad de las políticas públicas de protección de datos y ciberseguridad, y la inacción de las plataformas digitales tienen el potencial de contribuir a la expansión de estas prácticas. Frente a este escenario, se requieren respuestas integrales desde una perspectiva de derechos humanos: centradas en las personas, con mecanismos de rendición de cuentas y reparación, y especial atención a los sectores en situación de vulnerabilidad.

Este informe está dividido en cuatro secciones. La primera sección aborda la infraestructura de Telegram y explica las razones por las cuales se ha convertido en un espacio propicio para la compraventa ilegal de datos. La segunda detalla la metodología empleada en la investigación empírica. La tercera presenta los hallazgos, centrados en grupos y canales de tres países de la región: Brasil, Perú y Argentina. Además de identificar las dinámicas de las ventas observadas, se incluyen aspectos relevantes del contexto sociotécnico, político y legal de cada país. Finalmente, se ofrecen recomendaciones dirigidas principalmente a las autoridades nacionales de dichos países, aunque con pertinencia para toda región, en relación con los casos identificados y la necesidad de contar con marcos normativos e infraestructuras sólidas y autónomas de aplicación. Asimismo, se formulan propuestas a organismos regionales, considerando el carácter transfronterizo de las políticas de protección de datos y ciberseguridad, así como la alta probabilidad de que estas prácticas trasciendan a otros países latinoamericanos.

VOLVER AL ÍNDICE

2

TELEGRAM COMO MERCADO ILICITO

Telegram es una de las aplicaciones de mensajería instantánea más utilizadas a nivel global, con más de mil millones de personas usuarias[1]. Su crecimiento también ha sido acelerado en América Latina, donde países como Brasil, México y Colombia[2] lideran las descargas en la región. Lanzada en 2013 por los hermanos rusos Pavel y Nikolai Durov[3], inicialmente Telegram fue concebida como una alternativa segura y privada frente a otras plataformas, al presentarse como un espacio de comunicaciones sin vigilancia estatal.

A diferencia de otras aplicaciones, Telegram permite crear grupos de hasta 200,000 miembros y enviar archivos de hasta 2 GB. Su estructura está diseñada para facilitar la creación de espacios masivos de interacción, con escasos controles de moderación o restricción de contenido[4], lo que la convierte en un entorno propicio para la difusión de información a gran escala. Estas características no solo estimulan la conformación de comunidades y el intercambio masivo de enlaces, sino que también han hecho de Telegram una plataforma atractiva para múltiples usos, incluyendo los ilegales.

A diferencia de otras aplicaciones de mensajería, Telegram no cifra los mensajes de extremo a extremo por defecto; solo los "chats secretos" cuentan con esta protección, la cual debe activarse manualmente y no está disponible para grupos ni canales. Además, la plataforma almacena en sus servicios de nube conversaciones, metadatos y datos de personas usuarias (como nombre, número de teléfono, contactos y dirección IP). Estas limitaciones contradicen parcialmente su promesa de privacidad. Sin embargo, Telegram conserva el atractivo para quienes buscan cierto grado de anonimato en interacciones superficiales, ya que no exige mostrar el número de teléfono y permite operar únicamente con un nombre de usuario.

Más allá de la comunicación directa entre personas usuarias, Telegram facilita la interacción masiva a través de grupos y canales, cada uno con características diseñadas para distintos tipos de comunicación. Los grupos están diseñados para

1. Para más información, ver: **https://telegram.org/faq/es.**

2. Para más información, ver: **https://www.statista.com/statistics/1336855/telegram-downloads-by-country/**

3. Disponible en: **https://telegram.org/faq/es#p-quienes-son-las-personas-que-estan-detras-de-telegram**

4. El País (2024). Algo pasa con Telegram. Disponible en: **https://elpais.com/opinion/2024-08-26/algo-pasa-con-telegram.html**

la interacción en tiempo real entre múltiples personas, denominadas "miembros", quienes pueden participar activamente enviando mensajes, compartiendo archivos y viendo quién más integra el grupo. Estos pueden ser públicos, visibles desde el buscador de Telegram, o privados, accesibles solo mediante un enlace de invitación. Los canales, en cambio, están diseñados para la comunicación unidireccional: únicamente los administradores pueden publicar mensajes, mientras que quienes se unen actúan como "suscriptores". A diferencia de los grupos, las personas suscriptoras no pueden ver quienes más se encuentran en el canal, solo el número total de suscriptores.

Uno de los elementos centrales del ecosistema de Telegram –tanto en usos legítimos como ilícitos–es el uso de *bots*: programas automatizados capaces de ejecutar tareas sin intervención ni supervisión humana directa. Funcionan mediante comandos predefinidos, integrándose con bases de datos externas para entregar resultados al instante. Aunque originalmente fueron diseñados para mejorar la experiencia de las personas usuarias, (por ejemplo, moderando chats, enviando recordatorios o facilitando interacciones en canales informativos) en la práctica muchos de ellos han sido adaptados para fines ilícitos[5].

En el caso de la compraventa de datos personales, los *bots* permiten acceder rápidamente a información, incluyendo datos sensibles. Basta con escribir en el chat del *bot* un número de identidad, un nombre completo o un teléfono para recibir automáticamente su dirección, vínculos familiares, datos laborales, antecedentes judiciales o financieros. Esta automatización facilita el acceso y la circulación de información personal fuera de los marcos legales de protección, lo que incrementa los riesgos de uso indebido, suplantación de identidad o vulneración de derechos en contextos marcados por grandes brechas de seguridad institucional[6].

Ahora bien, teniendo en cuenta la temática de este informe, es importante mencionar que en los últimos años, Telegram ha estado vinculada a hechos de gran repercusión pública relacionados con actividades ilícitas. En agosto de 2024, Pavel Durov fue detenido[7] en París en el marco de una investigación sobre delitos facilitados por la plataforma, como la distribución de material de abuso sexual infantil y el tráfico de drogas. Pocos meses después, en noviembre del mismo año, una investigación[8] reveló el funcionamiento de un grupo con más de 70.000 hombres en Telegram que compartían estrategias para drogar y agredir sexualmente a mujeres.

5. Flare (2023). The Typology of Illicit Telegram Channels. Disponible en: **https://flare.io/wp-content/uploads/The-Typology-of-Illicit-Telegram-Channels.pdf**

6. Ibid

7. El Mundo (2024). El CEO de Telegram, Pavel Durov, arrestado en Francia. Disponible en: **https://www.elmundo.es/tecnologia/2024/08/25/66ca5dcffc6c83fe1b8b4594.html**

8. Público (2024). Una investigación destapa una red de hasta 70.000 hombres en Telegram que comparten estrategias para drogar y agredir sexualmente a mujeres. Disponible en: **https://www.publico.es/mujer/violencia-machista/investigacion-destapa-red-70-000-hombres-telegram-comparten-estrategias-drogar-agredir-sexualmente-mujeres.html**

Este episodio marcó un giro en la política histórica de Telegram de no cooperación con agentes estatales. Tras la detención de Durov, la plataforma anunció[9] que comenzaría a colaborar con autoridades bajo orden judicial, entregando datos como el número de teléfono o la dirección IP de las personas usuarias.

Casos como este refuerzan las preocupaciones sobre la postura pasiva de la plataforma frente a formas organizadas de violencia[10]. La existencia de herramientas de privacidad es fundamental para garantizar la libertad de expresión, la seguridad y la protección de las personas usuarias, especialmente en contextos de vigilancia o persecución política. Sin embargo, también resulta indispensable exigir a las empresas tecnológicas su deber de actuar ante los daños que se originan o se reproducen en sus entornos. Además de prevenir, deben asumir responsabilidades en la detección temprana, mitigación y reparación de los impactos que sus propias arquitecturas facilitan o amplifican.

Al igual que otras tecnologías orientadas a la protección de la privacidad, Telegram tiene el potencial de servir tanto para el resguardo legítimo de derechos como para facilitar abusos y perpetuar violencias. Este informe no busca descalificar prácticas ni espacios digitales que defienden la privacidad y el anonimato, ya que ambos constituyen derechos fundamentales y, a la vez, condiciones habilitantes para el ejercicio de otros derechos humanos en el entorno digital, como la libertad de expresión y de asociación. Es decir, la potencialidad de un doble uso no invalida la importancia de su existencia, pero sí exige un análisis crítico sobre cómo las decisiones de diseño, gobernanza y transparencia impactan en su uso cotidiano.

9. El Mundo (2024). Durov se rinde, Telegram comenzará a compartir datos con las autoridades. Disponible en: **https://www.elmundo.es/tecnologia/2024/09/24/66f2c8dde85ece674a8b457e.html**

10. Centro de Empresas y Derechos Humanos (2025). Violencia digital contra mujeres a través de redes sociales y la insuficiencia de los mecanismos de denuncia. Disponible en: **https://www.business-humanrights.org/es/%C3%BAltimas-noticias/m%C3%A9xico-violencia-digital-contra-mujeres-a-trav%C3%A9s-de-redes-sociales-por-parejas-y-exparejas-y-la-insuficiencia-de-los-mecanismos-de-denuncia/**

VOLVER AL ÍNDICE

3 METODOLOGÍA

La investigación se desarrolló entre octubre de 2024 y noviembre de 2025, con foco en Brasil, Perú y Argentina. El objetivo fue identificar las dinámicas de comercialización de datos personales a través de canales y grupos públicos de Telegram en América Latina, en contextos donde las desigualdades estructurales, la debilidad institucional y la escasa efectividad de protección de datos amplifican los riesgos para la ciudadanía.

El enfoque metodológico y el trabajo de campo se organizaron en tres fases principales: exploración, observación y análisis.

La fase de exploración permitió identificar los espacios públicos donde se realiza la compra y venta de datos dentro de Telegram. Para ello, se localizaron grupos y canales mediante cuatro estrategias: la aplicación de la técnica de muestreo de bola de nieve *(snowball sampling)*[11], herramientas de búsqueda automatizada y manual en Telegram, así como monitoreo de denuncias en redes sociales sobre la venta de datos personales.

Con respecto a las herramientas de búsqueda automatizada, se recurrió a una técnica de scrapping automatizado de contenido público mediante el desarrollo de scripts o códigos personalizados en Python[12]. Se emplearon palabras clave como "venta" o "datos" para identificar los grupos y canales potencialmente dedicados a la compra y venta de datos personales. Estas palabras también guiaron la búsqueda manual de los espacios en el buscador de Telegram.

El monitoreo de denuncias en redes sociales, por su parte, permitió reconocer enlaces que llevaban a grupos públicos de Telegram relacionados con la venta de datos, al igual que visibilizar narrativas de las personas usuarias sobre la exposición de sus datos personales y las consecuencias derivadas.

11. La aplicación de esta técnica consistió en rastrear enlaces compartidos dentro de los propios grupos identificados. Al seguir esas conexiones, se descubrieron otros espacios similares. En varios casos, un canal conducía a varios más, permitiendo construir una red amplia de observación. Esta estrategia resultó ser la más efectiva para localizar la mayoría de los grupos y canales analizados.

12. Jünger, J. (2023). Scraping social media data as platform research: A data hermeneutical perspective. In C. Strippel, S. Paasch-Colberg, M. Emmer, & J. Trebbe (Eds.), Challenges and perspectives of hate speech research (pp. 427-441). Berlin **https://doi.org/10.48541/dcr.v12.25**

Una vez identificados los espacios, se desplegó una técnica de observación no participante[13] de las dinámicas durante los meses de investigación, tanto mediante monitoreo en tiempo real (capturando las interacciones entre vendedores y compradores, así como los mensajes promocionales, respuestas automáticas y comportamientos de consulta), como mediante la revisión del historial de mensajes, detallando tendencias, estructuras organizativas y cambios en los métodos de comercialización.

Por último, tras la saturación de la información se realizó el análisis de los datos recopilados, a partir de la construcción de una bitácora comparativa con criterios que incluían: el alcance de los grupos y canales, sus administradores, los tipos de datos comercializados, el modelo de negocio, los precios y los métodos de pago.

Durante la fase de análisis, se realizó una investigación documental para profundizar en los contextos tecnopolíticos, sociales y legales de Brasil, Perú y Argentina en materia de protección de datos personales. Este trabajo permitió identificar, entre otros elementos, los marcos regulatorios vigentes y los historiales de filtraciones de datos en instituciones públicas de estos países.

Al tratarse de una investigación sobre dinámicas ilegales de compra y venta, se adoptaron medidas para proteger la seguridad tanto de las personas cuyos datos pudieron verse comprometidos como de quienes realizaron el trabajo de investigación. En ese marco, se aplicaron los siguientes principios:

No se incluye en este reporte nombres ni enlaces de grupos o canales para evitar la reproducción del daño.

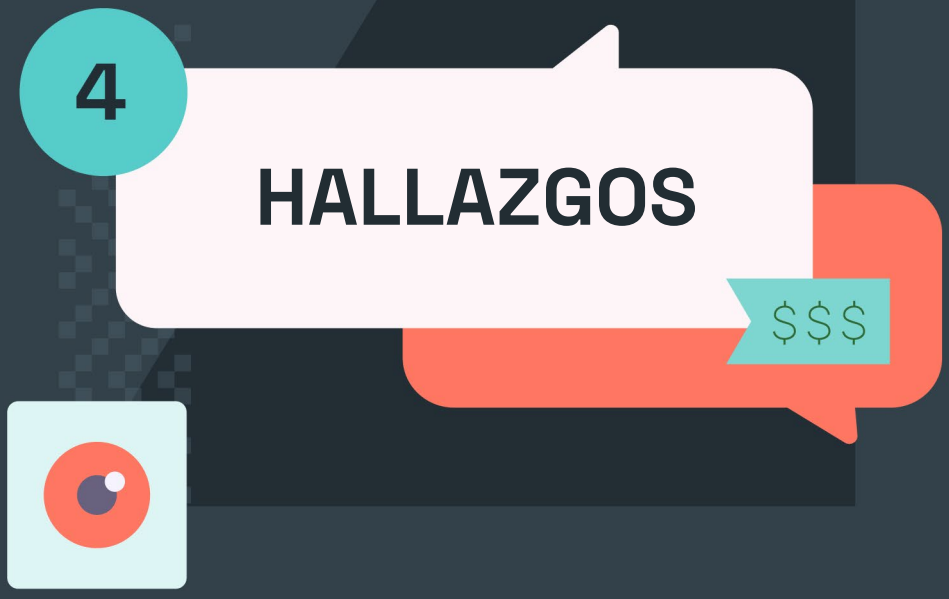
La investigación fue de carácter no participante: no se estableció contacto con administradores de los espacios ni compradores, evitando cualquier forma de interacción directa.

Se desactivó la descarga automática de archivos, ya que durante la exploración se detectaron espacios con contenido violento y sexual.

13. Hine, C. (2015). Ethnography for the Internet: Embedded, Embodied and Everyday. Disponible en: **https://www.taylorfrancis.com/books/mono/10.4324/9781003085348/ethnography-internet-christine-hine**

VOLVER AL ÍNDICE

4 HALLAZGOS



La investigación se centró en veinte y siete espacios activos dedicados a la comercialización de datos personales en Telegram distribuidos entre Brasil, Perú y Argentina. Durante el trabajo de campo se constató que en varios grupos y canales dedicados a la venta de datos en estos países también circulaba información correspondiente a otros territorios, como Venezuela, Bolivia, República Dominicana, Chile y Uruguay, lo que sugiere que se trata de un fenómeno regional más amplio que excede los tres países analizados en detalle. Sin embargo, el análisis que sigue se concentra en los hallazgos principales de Brasil, Perú y Argentina.

Estos veinte y siete espacios fueron clasificados según el país de origen, el tipo de interacción (grupo o canal) y el idioma utilizado para la comunicación:

Tabla 1. Descripción de los espacios observados

País	Grupos	Canales	Idioma
Brasil	10	0	Portugués
Perú	8	2	Español
Argentina	1	6	Español

Es importante señalar que esta cifra no representa la totalidad de grupos y canales utilizados para la venta de datos en Telegram, sino una muestra intencional definida según criterios de accesibilidad, actividad sostenida y observación segura, ética y no intrusiva[14]. Se priorizó el análisis de aquellos espacios que permitieran una evaluación comparativa sin comprometer la seguridad de las personas usuarias ni de quienes realizaron la investigación.

4.1 Brasil

En Brasil se identificaron diez grupos, varios de ellos con un número considerable de miembros, lo que revela un alto nivel de tráfico y permanencia:

14. Ibid

Tabla 2. Número de miembros de los grupos observados

Grupo1	Grupo2	Grupo3	Grupo4	Grupo5
39.155	33.333	34.403	11.882	9.587

Grupo6	Grupo7	Grupo8	Grupo9	Grupo10
35.982	690	24.775	47.356	10.031

En estos grupos, se observó un elevado grado de automatización en la gestión. Todos los espacios analizados cuentan con al menos un configurado como administrador, lo que garantiza una atención constante a las solicitudes de datos, sin necesidad de intervención y supervisión humana permanente. Esta estructura facilita el funcionamiento del grupo como una tienda activa las 24 horas, con comandos operativos preestablecidos para realizar búsquedas o compras.

A la par de los *bots*, se identificó la presencia de administradores humanos que operan bajo una jerarquía reconocible. Se utilizan etiquetas como "*Dono*" (dueño), "*admin*", "*suporte*" (soporte) o "*help*" (ayuda), que permiten delimitar funciones dentro del espacio. La gestión no parece centralizada en una única persona, sino articulada por un equipo. Se observó que ese equipo opera de manera anónima a través del uso de esos seudónimos genéricos y la fragmentación de responsabilidades. Así, la coordinación se da en la medida que cada rol cumple una función específica sin necesidad de revelar identidades, dificultando el rastreo.

El modelo de negocio predominante identificado en los grupos es el *freemium,* donde las personas usuarias pueden realizar una cantidad limitada de consultas gratuitas usando *bots* en Telegram, las cuales suelen arrojar resultados básicos (por ejemplo, nombre y CPF[15]). Sin embargo, para acceder a datos más detallados, como dirección, fechas de nacimiento, vínculos laborales o información financiera, es necesario pagar.

Los grupos ofrecen diferentes planes según el tiempo de acceso (diario, semanal, mensual, trimestral, etc.) y, en algunos casos, por niveles de funcionalidad referentes al tipo de dato consultado. Este enfoque se asemeja a un modelo *freemium* escalonado, donde se accede gratuitamente a funcionalidades limitadas y se incentiva el pago para obtener consultas más detalladas. Los precios mínimos identificados oscilan entre $1 USD (por una semana) y $78.80 USD (por dos años). Se identificaron promociones y anuncios de urgencias de compra (por ejemplo "solo por hoy"), lo que refleja el uso de estrategias típicas del marketing digital adaptadas a un mercado ilícito.

En cuanto al método de pago, todos los grupos analizados utilizan el sistema PIX, un mecanismo de pago instantáneo lanzado por el Banco Central de Brasil en 2020[16]. Este sistema permite realizar transferencias en tiempo real entre personas o empresas, utilizando identificadores únicos (como número de teléfono, correo electrónico, CPF o códigos QR), sin necesidad de intermediarios bancarios tradicionales. Si bien

15. CPF equivale a "Cadastro de Pessoa Física", es decir, el número de identificación fiscal en Brasil.

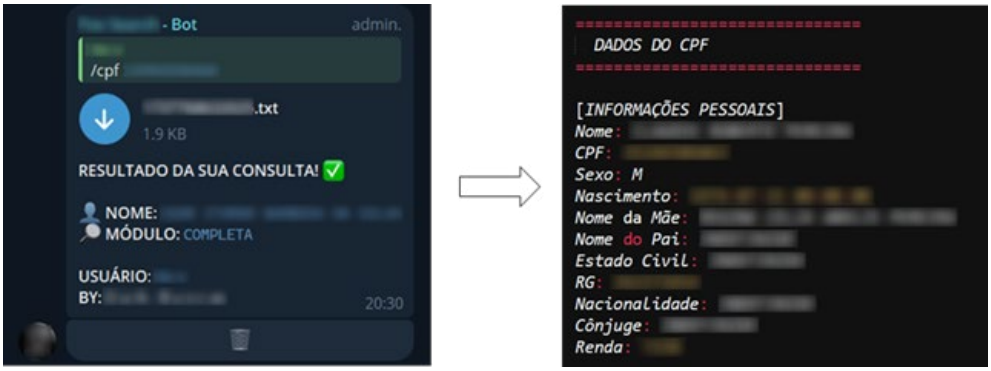
16. Para más información, ver: **https://www.bcb.gov.br/estabilidadefinanceira/pix**

el PIX fue diseñado para garantizar la trazabilidad y reducir los costos de las transacciones, su uso en entornos informales muestra cómo herramientas financieras legítimas pueden ser aprovechadas para operaciones ilícitas o fuera de regulación. En los grupos analizados, los pagos en general se ejecutan mediante un código aleatorio generado a través de plataformas intermediarias, como **iugu.com**, que integran soluciones de facturación electrónica.

Se observó un uso intensivo de *bots* automatizados para la venta de datos personales. El comando más frecuente es **/cpf,** el cual permite consultar información vinculada al número de identificación fiscal en Brasil. Al ingresar este comando seguido del número de CPF de la persona, el *bot* genera una ficha estructurada que puede descargarse en formato .txt, la cual revela los datos personales vinculados al CPF de manera inmediata.

Los datos proporcionados a través del comando **/cpf** configuran un perfil extremadamente detallado de la persona consultada (ver Imagen 1). En primer lugar, se incluye información de identificación civil: nombre completo, RG (Registro Geral), fecha de nacimiento, sexo[17], municipio y estado de origen. El registro de CPFs es administrado por la **Receita Federal do Brasil,** entidad encargada de la gestión fiscal y tributaria y responsable de la base nacional de contribuyentes.

Imagen 1. Evidencia visual sobre venta de datos a través del comando **/cpf**



La ejecución del comando también ofrece acceso a información económica, como la estimación de la renta mensual de la persona consultada. Además, se incluye una categorización del poder adquisitivo expresado en niveles («bajo», «medio» o «alto») junto con una banda monetaria que indica el rango de ingresos estimados. Esta clasificación puede provenir de registros tributarios o de consumo, y puede usarse para inferir la situación socioeconómica de la persona afectada, exponiéndola a riesgos de discriminación, estigmatización y prácticas de exclusión o de búsqueda por ventaja financiera.

Junto con los datos económicos, el archivo revela un sistema de *scoring* financiero, es decir, un sistema que clasifica a la persona según su nivel de riesgo crediticio.

17. A lo largo de este reporte se hace referencia tanto al dato "sexo" como a "género". Esta variación responde a la forma en que la información aparece en cada grupo o canal analizado en Telegram, y al modo en que los programadores de cada *bot* definen las variables dentro de sus sistemas de consulta. Por ello, se mantienen ambos términos conforme a su uso original en las fuentes observadas.

Este sistema utiliza modelos como CSB[18] y CSBA[19], donde se asignan puntuaciones cualitativas. La presencia de estas métricas específicas sugiere que los *bots* estarían accediendo, presuntamente, a bases de datos crediticias institucionales, como SERASA[20] o SPC Brasil[21], permitiendo construir perfiles financieros detallados sin el consentimiento de la persona titular.

El perfil financiero de la persona consultada parece complementarse con información extraída presuntamente del sistema SERASA MOSAIC, una herramienta utilizada en Brasil para segmentar consumidores según su comportamiento y capacidad de consumo[22]. En los registros analizados, se incluye la descripción del perfil, la clase socioeconómica, distintos códigos de categorización ("nuevo", "secundario", "principal") y observaciones adicionales que podrían estar vinculadas a su historial de compras, pagos o deudas –justamente campos como los disponibles en el propio sistema SERASA MOSAIC–.

Se encontró que, a través de este mecanismo de consulta también es posible acceder a información financiera vinculada al ámbito laboral de las personas. El comando revela la profesión declarada, junto con el código CBO (Código Brasileiro de Ocupações), una clasificación oficial utilizada en Brasil para estandarizar actividades laborales. Además, los *bots* acceden a información laboral altamente detallada como aquella que se encuentra en registros oficiales como los de la tarjeta de trabajo y seguridad social (Carteira de Trabalho e Previdência Social - CTPS), por dar un ejemplo. Así, la estructura de los datos coincide con los campos presentes en dichos registros: múltiples entradas laborales por persona, nombre de la empresa empleadora, identificación tributaria (CNPJ), municipio y estado, fechas de ingreso, cargo, salario mensual, grado de instrucción e incluso variables censales como raza y sexo (ver Imagen 2). Estos elementos permiten identificar con precisión el rubro profesional de la persona.

18. CSB (Credit Score Básico): Indicador utilizado en Brasil que califica el riesgo crediticio de una persona en función de variables básicas, como historial de pagos y deudas registradas.

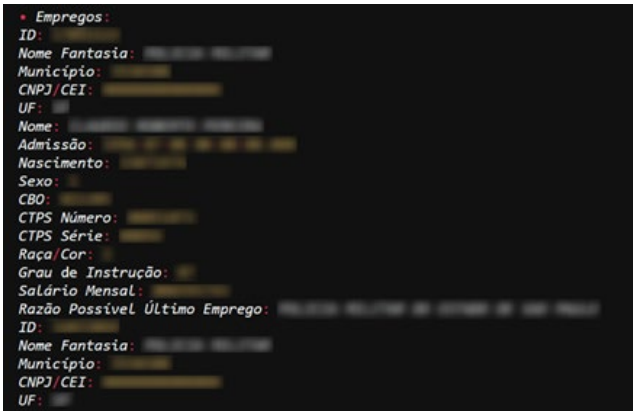
19. CSBA (Credit Score Básico Ampliado): Variante del CSB que incorpora más variables, incluyendo información de comportamiento de consumo y relaciones con instituciones financieras, proporcionando un análisis crediticio más completo.

20. SERASA: Empresa brasileña de análisis y gestión de datos financieros, reconocida por operar una de las principales bases de datos crediticias del país, utilizada por entidades para evaluar la solvencia de consumidores.

21. SPC Brasil (Servicio de Protección al Crédito): Sistema crediticia gestionado por las cámaras de comercio brasileñas, que centraliza datos sobre deudas, pagos y comportamiento crediticio de personas naturales y jurídicas.

22. Disponible en: **https://www.serasaexperian.com.br/solucoes/mosaic/**

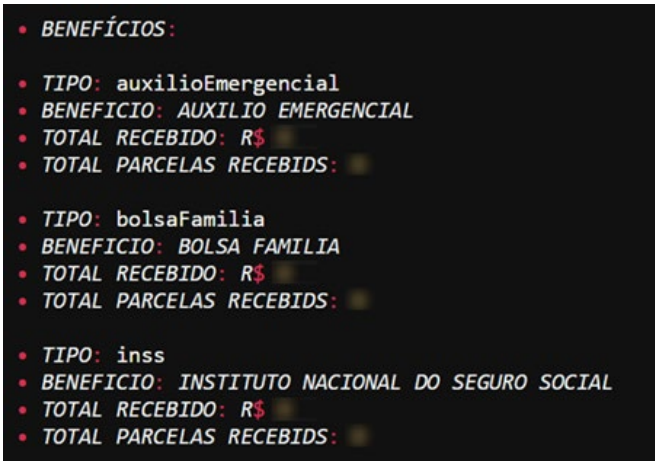
Imagen 2. Evidencia visual sobre venta de datos con información laboral



En varios de esos registros laborales, la fecha de salida aparece como *"null"*, lo que podría indicar que la persona aún trabaja en esa empresa o que el sistema de origen no ha actualizado ese campo. Sin embargo, lo más relevante es que el uso del término *"null"* es característico de bases de datos estructuradas, como aquellas basadas en SQL[23], lo que sugiere que la información proviene de sistemas o respaldos de bases de datos y no de simples capturas o recolecciones informales.

Se encontró, como dato altamente sensible, la exposición del número PIS (Programa de Integração Social), un identificador clave para acceder a beneficios estatales como pensiones, subsidios y fondos de retiro. A ello, se suma información detallada sobre acceso a beneficios sociales como el Auxílio Emergencial (beneficio otorgado en pandemia), Bolsa Família (histórico programa de transferencia de renta) y aportes del INSS (Instituto Nacional do Seguro Social). En cada caso se especifica el monto total recibido por la persona y la cantidad de cuotas entregadas, lo que permite trazar patrones de asistencia social (ver Imagen 3). Esta información no solo expone el nivel de vulnerabilidad económica de la persona, sino que también permite inferencias sobre su situación laboral, historial de ingresos y grado de dependencia de programas estatales, exponiéndola potencialmente a fraudes dirigidos y a discriminación.

Imagen 3. Evidencia visual sobre venta de datos con información de acceso a beneficios sociales



23. SQL (Structured Query Language) es un lenguaje estándar utilizado para gestionar bases de datos estructuradas, permitiendo consultar y actualizar la información almacenada.

La estructura de estas fichas de datos proporcionadas por los *bots* de los grupos analizados tiene campos como "tipo: auxilioEmergencial" y "beneficio: AUXILIO EMERGENCIAL". Ello evidencia una nomenclatura propia de bases de datos, caracterizada por el uso de etiquetas en formato "campo:valor" y por convenciones técnicas como el *camelCase*[24] ("auxilioEmergencial"). Aquí, una vez más, estas características sugieren que la información podría haber sido extraída directamente desde bases de datos estructuradas, posiblemente filtradas o conectadas en tiempo real, del sistema financiero o de protección social.

El mismo archivo de consulta a través del CPF también revela líneas de teléfono móvil asociados a la persona consultada. Para cada línea, se indica el tipo de servicio y la operadora de telecomunicaciones correspondiente. La aparición de múltiples registros asociados a una misma persona podría deberse a un cruce de bases de datos, posiblemente provenientes de proveedores de servicios móviles o registros históricos de líneas activas e inactivas.

El acceso a domicilios registrados constituye otra dimensión crítica de la exposición de datos. En el mismo archivo.txt de respuesta, se identifican múltiples registros por persona, lo que indica que las bases almacenan un historial de direcciones a lo largo del tiempo. Cada entrada contiene información granular como el código postal (CEP), estado federativo (UF), municipio, calle (logradouro), barrio (bairro), número de residencia y complemento, permitiendo ubicar a una persona con alta precisión geográfica. Además del domicilio actual, se incluye el municipio de nacimiento, lo que amplía la trazabilidad del recorrido vital de la persona.

La exposición de múltiples domicilios permite rastrear movimientos pasados y presentes, lo que puede derivar en riesgos de acoso, extorsión o vigilancia. En contextos como el brasileño –y, en general, en varios países de América Latina– donde convergen altos niveles de violencia urbana, crimen organizado, desigualdad y polarización política[25], este tipo de filtraciones puede exponer a las personas a amenazas diversas: desde fraudes direccionados y agresiones físicas o digitales hasta hostigamientos direccionados, motivados por razones políticas, de género o de pertenencia étnica, entre otros.

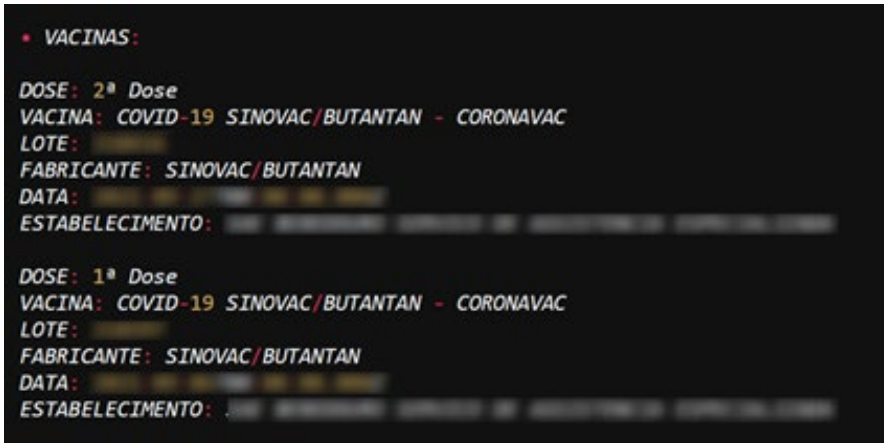
La exposición no se limita a la persona consultada. En los registros analizados se visualiza también información sobre su red familiar directa (como hermanas, hermanos, sobrinas, sobrinos) y otros vínculos de parentesco. Cada familiar aparece identificado por su nombre completo y número de CPF. Asimismo, bajo la etiqueta *"vizinhos"* (vecinos), los *bots* divulgan datos de personas que residen en las proximidades del titular consultado. La inclusión de estos terceros amplía el alcance de la filtración y podría facilitar la elaboración de perfiles relacionales, capaces de mapear vínculos familiares y comunitarios, y eventualmente combinarse con otros datos para fines como fraudes dirigidos, suplantación de identidad, extorsión o vigilancia por actores no estatales.

24. Convención de escritura en informática donde la primera palabra se escribe en minúscula y las siguientes comienzan con mayúscula, sin espacios ni guiones.

25. WOLA (2011). Enfrentando la violencia urbana en América Latina: Revirtiendo la exclusión a través de la actuación policial inteligente y la inversión social. Disponible en: **https://www.wola.org/sites/default/files/downloadable/Citizen%20Security/2011/Enfrentando_la_Violencia_Urbana.pdf**

Otro hallazgo alarmante en dicho archivo de texto es la exposición del historial de vacunación, donde se presentan datos estructurados que replican la lógica de un registro oficial del sistema de salud brasileño como aquel del Sistema Único de Salud (SUS), lo que señalaría un posible acceso o filtración de fuentes estatales. Se detalla el tipo de dosis (primera o segunda), el nombre de la vacuna administrada, el número de lote, el fabricante, la fecha exacta de aplicación y el establecimiento de salud donde fue suministrada (ver Imagen 4). Además de constituir una grave afectación a la privacidad, este tipo de información puede prestarse a distintos usos indebidos, entre ellos la falsificación de certificados sanitarios o la suplantación de identidad para acceder a servicios médicos.

Imagen 4. Evidencia visual sobre venta de datos con el historial de vacunación.



Además del comando **/cpf,** que requiere el número de identificación de la persona, los *bots* también permiten ejecutar el comando **/nome,** o sea, buscar las fichas de datos personales en venta de alguien a través de su nombre y apellido, sin necesidad de conocer su CPF. El *bot* responde con una lista de coincidencias que incluyen nombre completo, número de CPF, género y fecha de nacimiento.

En los grupos investigados también es posible consultar datos personales a partir de números de celular y placas de vehículos. Además, el comando **/cnpj** permite acceder a información detallada sobre personas jurídicas (empresas, fundaciones u asociaciones) mediante su número de identificación fiscal. La consulta devuelve una ficha con datos como la razón social (nombre legal de la empresa), el nombre comercial, la naturaleza jurídica (asociación civil, sociedad anónima o cooperativa), la situación actual de la empresa (“activa” o “inactiva”), la fecha de apertura, el capital social declarado y el tamaño de la empresa, categorizado según su porte (micro, pequeña, mediana, etc.).

4.1.1 Contexto tecnopolítico y legal

De acuerdo con la empresa global de ciberseguridad Surfshark, en 2024, Brasil ocupó la séptima posición en el ranking mundial de filtraciones de datos[26]. Esto evidencia que los incidentes de filtración no son nuevos ni escasos en el país y pueden haber contribuido a alimentar y habilitar el mercado ilegal de información personal. Uno de los casos más emblemáticos de filtración de información ocurrió en 2021, cuando se expusieron datos de más de 223 millones de personas, incluyendo el número de CPF, nombre, fecha de nacimiento y género. La cifra supera a la población total de Brasil, lo que indica que también se vieron comprometidos registros de personas fallecidas[27].

La magnitud de las filtraciones en Brasil debe analizarse considerando un ecosistema digital caracterizado por el uso masivo de aplicaciones de mensajería y redes sociales[28], así como por altos índices de fraude y criminalidad digital. Según datos del Senado Federal, uno de cada cuatro brasileños con más de 16 años reportó haber sido víctima de un ataque digital en 2023[29], y estudios recientes estiman pérdidas anuales superiores a los 70 mil millones de reales (lo que equivale a casi 13 mil millones de USD en octubre de 2025) por fraudes financieros y robos de datos de personas brasileñas[30]. Este contexto combina una penetración tecnológica muy elevada con bajos niveles de alfabetización digital y una creciente sofisticación de los mecanismos de estafa y suplantación de identidad[31].

En ese marco, el uso de Telegram –una de las aplicaciones más populares del país– ha estado acompañado de tensiones con las instituciones nacionales en torno a la circulación de información ilícita y al incumplimiento de decisiones judiciales. En marzo de 2022, el Supremo Tribunal Federal (STF) ordenó la suspensión temporal de la plataforma por la falta de cooperación con el sistema de justicia[32]. La medida fue revertida dos días después, tras el compromiso de la empresa de designar un representante legal en el país, cumplir con órdenes judiciales y establecer meca-

26. Para más información, ver: **https://surfshark.com/research/data-breach-monitoring?country=-br**

27. andro4all (2024). Una filtración masiva expone los datos de 223 millones de personas: la población de Brasil al completo. Disponible en: **https://andro4all.com/tecnologia/una-filtracion-masiva-expone-los-datos-de-223-millones-de-personas-la-poblacion-de-brasil-al-completo**

28. Folha de S. Paulo (2023). Brasil é o país do WhatsApp, diz presidente do aplicativo. Disponible en: **https://www1.folha.uol.com.br/mercado/2023/11/brasil-e-o-pais-do-whatsapp-diz-presidente-do-aplicativo.shtml**

29. Agência Senado (2024). Golpes digitais atingem 24% da população brasileira, revela DataSenado. Disponible en: **https://www12.senado.leg.br/noticias/materias/2024/10/01/golpes-digitais-atingem-24-da-populacao-brasileira-revela-datasenado**

30. Folha de S. Paulo (2024). fraude e roubo dão prejuízo de R$ 71 bi - UOL. Disponible en: **https://www1.folha.uol.com.br/cotidiano/2024/08/fraude-digital-e-roubo-de-celular-dao-prejuizo-de-r-71-bi-em-1-ano-aponta-datafolha.shtml**

31. WOMCY (2025). Brasil na mira: por que o país é tão visado por ataques cibernéticos? Disponible en: **https://womcy.org/pt/brasil-na-mira-por-que-o-pais-e-tao-visado-por-ataques-ciberneticos/**

32. Supremo Tribunal Federal (2022). Ministro Alexandre de Moraes suspende funcionamento do Telegram no Brasil. Disponible en: **https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=483659&ori=1**

nismos de cooperación con el Tribunal Superior Electoral (TSE)[33].

Frente a este escenario de vulneración de datos y riesgos crecientes, resulta clave considerar el marco normativo vigente en Brasil. El país cuenta con la Ley nº 13.709 – Ley General de Protección de Datos Personales (LGPD por sus siglas en portugués), sancionada en 2018 y vigente desde 2020[34]. La norma regula el tratamiento de datos personales, incluyendo en medios digitales, tanto por personas físicas como jurídicas, públicas o privadas, con el objetivo de proteger derechos fundamentales de libertad, privacidad y el libre desarrollo de la personalidad. Entre sus principios figuran la seguridad, la prevención y la no discriminación.

La LGPD define como datos sensibles aquellos relativos a "origen racial o étnico, convicción religiosa, opinión política, afiliación sindical, salud, vida sexual, datos genéticos o biométricos vinculados a una persona". Considerando esta definición, información como los historiales de vacunación –que circulan en los mercados ilegales de Telegram– constituye información sensible. La normativa establece para estos casos obligaciones más estrictas, incluyendo medidas específicas de seguridad de la información.

Asimismo, la ley dedica un capítulo al tratamiento de datos por parte de órganos públicos, aunque sin establecer reglas muy diferenciadas o rigorosas. Entre sus disposiciones más relevantes se encuentra la posibilidad de que, en casos de infracciones cometidas por organismos estatales, la Agencia Nacional de Protección de Datos (Agência Nacional de Proteção de Dados - ANPD) emita recomendaciones destinadas a cesar la violación. Esto indicaría que, de comprobarse alguna vinculación entre la circulación indebida de datos personales en los grupos de Telegram y la responsabilidad estatal en el manejo o resguardo de datos, el órgano tendría facultades para intervenir el plano administrativo para mitigar los daños y promover medidas de reparación específicas al caso.

La ANPD fue creada en 2019, inicialmente bajo la estructura de la Presidencia de la República, sin independencia efectiva[35]. En 2022 adquirió la naturaleza de autarquía especial, pasando a estar vinculada al Ministerio de Justicia y Seguridad Pública. Sin embargo, continuó enfrentando limitaciones de recursos humanos y financieros[36] y su actuación sancionadora ha sido hasta el momento tímida. Muy recientemente, en septiembre de 2025, con la Medida Provisoria 1.317/2025[37], la ANPD fue transformada oficialmente en agencia reguladora, dejando de estar subordinada al Ministerio y obteniendo total autonomía técnica, funcional, administrativa y decisoria. Esta reforma institucional creó también nuevos cargos especializados y refuerzó

33. Supremo Tribunal Federal (2022). Ministro Alexandre de Moraes revoga bloqueio após Telegram cumprir determinações do STF
Disponible en: **https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=483712&ori=1**

34. Disponible en: **https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm**

35. Para más información, ver: **https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm**

36. tele.síntese (2023). Em aniversário de 3 anos, ANPD reivindica estrutura proporcional ao desafio.
Disponible en: **https://telesintese.com.br/em-aniversario-de-3-anos-anpd-reivindica-estrutura-proporcional-ao-desafio/**

37. Disponible en: **https://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2025/Mpv/mpv1317.htm**

su capacidad operativa, lo que puede ampliar su margen de acción futura ante vinculaciones estatales en casos de tratamiento indebido de datos.

En paralelo, el Código Penal brasileño tipifica desde 2012 la intrusión del dispositivo informático, con penas de uno a cuatro años de prisión y multa. Las sanciones para el delito son agravadas cuando ésta resulta en obtención y comercialización de datos, especialmente si involucra organismos públicos o servicios financieros, situaciones que podrían guardar relación con las prácticas descritas en este informe[38].

En materia de ciberseguridad, Brasil adoptó en agosto de 2025 su nueva Estrategia Nacional de Ciberseguridad (E-Ciber), que actualiza la anterior de 2020[39]. La estrategia está estructurada bajo los ejes temáticos de protección y conscientización de la ciudadanía; seguridad y resiliencia de los servicios esenciales e infraestructuras críticas; cooperación e integración entre los órganos y entidades públicas y privadas; y soberanía nacional y gobernanza. Entre las acciones previstas se incluye el incentivo a la expansión de servicios de apoyo a víctimas de ilícitos cometidos en espacios digitales.

En 2023, aún bajo la vigencia de la Estrategia anterior, se creó el Comité Nacional de Ciberseguridad (CNCiber). Este órgano colegiado, presidido por el Gabinete de Seguridad Institucional de la Presidencia de la República, reúne a representantes del gobierno, la academia, el sector privado y la sociedad civil. Su mandato incluye proponer actualizaciones a la estrategia, formular medidas para prevenir y responder a incidentes y promover la cooperación internacional en la materia[40].

En síntesis, Brasil cuenta con una arquitectura legal e institucional relativamente robusta, que incluye una ley moderna de protección de datos, un marco penal específico para delitos informáticos y una estrategia nacional de ciberseguridad. Sin embargo, la escasa cultura de protección de datos y de ciberseguridad, sumada a la limitada capacidad operativa de la ANPD y su reciente independencia, reducen la efectividad de los marcos vigentes. En un país de dimensiones continentales, marcado por un historial recurrente de filtraciones masivas y fraudes digitales, se amplifican los riesgos para la ciudadanía.

38. Para más información, ver: **https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm**

39. Disponible en: **https://www2.camara.leg.br/legin/fed/decret/2025/decreto-12573-4-agosto-2025-797813-publicacaooriginal-176048-pe.html**

40. Para más información, ver: **https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/D11856.htm**

4.2 Perú

En Perú se analizaron ocho grupos y dos canales de Telegram. Los grupos presentan un alcance amplio en relación con la extensión del país, mientras que los canales tienen una base de suscriptores mucho menor:

Tabla 3. Número de suscriptores de los canales observados

Grupo1	Grupo2	Grupo3	Grupo4	Grupo5
8.698	3.109	915	539	12.847

Grupo6	Grupo7	Grupo8	Canal1	Canal2
2.395	1.280	3.390	71	74

Al igual que en Brasil, se identificaron *bots* con funciones de administración, encargados de responder consultas o ejecutar búsquedas. En paralelo, los administradores humanos parecen mantener estructuras jerárquicas con denominaciones como *"owner", "founder", "admin",* "moderador" o *"dev"*, replicando el esquema funcional de muchas comunidades digitales formales.

Un elemento socialmente significativo observado en algunos grupos fue el uso de lenguaje discriminatorio en los roles asignados, con nombres como "Gato Gay" o "Cabro" (término despectivo en jerga local) atribuidos a cuentas administradoras. Estas denominaciones reflejan un imaginario marcado por lógicas machistas, LGBTQIA+-fóbicas y excluyentes en general, comunes en entornos altamente masculinizados, que normalizan la burla respecto a identidades diversas. Su presencia revela que, más allá de la estructura técnica, estos espacios también reproducen dinámicas sociales de discriminación basadas en género y orientación sexual.

El modelo de negocio predominante en Perú también es el *freemium,* aunque con ciertas diferencias respecto de Brasil. En algunos grupos, el *bot* permite realizar búsquedas gratuitas, pero los resultados aparecen parcialmente ocultos: se muestran nombres y apellidos, mientras que el resto de los datos personales (como fecha de nacimiento, dirección y edad) aparecen reemplazados por asteriscos (***). Para desbloquear esta información, el *bot* sugiere comprar créditos. Este modelo genera una experiencia de "prueba parcial" que motiva la compra.

La mayoría de los grupos opera bajo una lógica de cobro por funcionalidad –por ejemplo, con funciones básicas y funciones Pro o VIP–, aunque también se hallaron planes basados en periodos de tiempo (por días o meses). Los precios oscilan desde $2.20 USD por acceso de tres días hasta montos anuales como $116.20 USD, siendo este último uno de los valores más altos registrados en toda la investigación. Asimismo, existen paquetes que se ofrecen con créditos, lo que permite acumular saldo virtual para distintas consultas. La presentación de planes en niveles (Básico, Estándar y Premium) sugiere una estrategia de escalamiento de beneficios vinculada al pago, en una lógica similar a la de plataformas legítimas de servicios digitales.

Los métodos de pago más comunes son las billeteras digitales Yape y Plin, ampliamente utilizadas a nivel nacional en Perú. Ambas plataformas permiten enviar di-

nero con tan solo un número de celular o un código QR, sin necesidad de conocer el nombre o número de cuenta bancaria de la persona destinataria. Si bien estas billeteras digitales permiten cierto nivel de trazabilidad, ya que el nombre completo del titular aparece al momento de realizar la transferencia, su uso sigue siendo frecuente en los mercados ilegales observados.

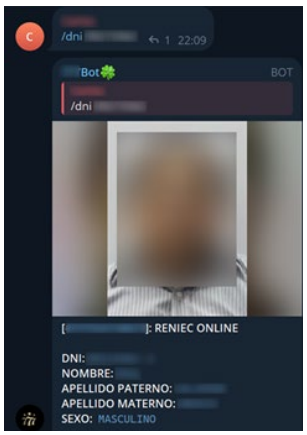
El comando más común para consultar y comprar datos en los grupos y canales peruanos es **/dni**, el cual permite acceder a una gran variedad de datos de cualquier persona ciudadana a partir de su Documento Nacional de Identidad (DNI). El DNI es el número único de identificación asignado a cada persona en Perú por la RENIEC[41], que actúa como entidad oficial encargada.

Tras este tipo de consulta, se observó que los *bots* generan en segundos una respuesta automática con una ficha de datos personales detallados, que deberían encontrarse únicamente en los registros oficiales. Esto sugiere un posible acceso indebido a bases de datos del Estado o la filtración de estos registros por parte de actores maliciosos. La respuesta incluye nombres completos (nombre, apellido paterno y materno), sexo y fecha de nacimiento. Además, se incluyen datos sobre el lugar de nacimiento, tales como departamento, provincia y distrito.

Otros campos revelan detalles adicionales como el estado civil, el grado de instrucción, la estatura, y diversas fechas clave: inscripción, emisión, caducidad del DNI y en algunos casos hasta la fecha de fallecimiento de la persona. También se reporta si la persona es donante de órganos. A nivel familiar, se listan los nombres y números de DNI del padre y la madre. El sistema también proporciona información completa sobre el domicilio registrado, incluyendo departamento, provincia, distrito y dirección.

A diferencia de Brasil, la respuesta automatizada incluye datos biométricos como huellas dactilares de las personas, incrementando exponencialmente el nivel de exposición y vulnerabilidad de los derechos afectados. En algunos casos, la fotografía se acompaña también de la firma manuscrita de las personas (ver Imagen 5).

Imagen 5. Evidencia visual sobre venta de datos a través del comando **/dni**



41. RENIEC (Registro Nacional de Identificación y Estado Civil): organismo autónomo del Estado peruano encargado de la identificación de las personas naturales, la emisión del Documento Nacional de Identidad (DNI) y la gestión del registro civil. Administra una de las principales bases de datos personales del país, incluyendo nombres, fechas de nacimiento, domicilios y datos biométricos.

Además, se observó que los *bots* en los grupos y canales peruanos también permiten obtener imágenes completas del DNI, tanto en su formato electrónico como en su versión física o virtual; incluso de niñas, niños y adolescentes. Para ello, emplean comandos como **/dniel** para el DNI electrónico (DNIe) y **/dniv** o **/dnivir** para el DNI azul o virtual, recibiendo archivos digitales en formato imagen (.jpg o .png) con la parte frontal y posterior del documento. En el caso del comando **/dniel**, los resultados muestran el DNI electrónico completo de una persona adulta, que cuenta con un chip integrado y es utilizado, entre otras cosas, para firmar documentos digitalmente.

Resulta especialmente preocupante la calidad de los documentos descargados observada, en tanto es suficientemente alta como para ser utilizados en falsificaciones, clonación de identidad, acceso a servicios bancarios o cualquier trámite digital. Además de los datos biométricos, el documento incluye información detallada (como nombres, apellidos, sexo, fecha y lugar de nacimiento), grado de instrucción, estado civil, estatura, nombre del padre y/o madre, dirección completa, y situación registral.

En algunos casos, las fotografías y fichas de datos presentan distintivos de órganos oficiales del Estado peruano. Aunque no puede determinarse con certeza el origen de los datos comercializados, la presencia de marcas, formatos y codificaciones coincidentes con los utilizados por entidades públicas genera alarmas sobre un posible acceso indebido a bases de datos oficiales o la filtración de documentos procesales. Un indicio particularmente relevante aparece en las fichas de tipo C4[42], donde figura un apartado titulado "Información de la consulta", que detalla quién realizó la búsqueda (nombre de usuario), desde qué entidad y con qué número de transacción. Este tipo de registro apunta a la posibilidad de que, en algunos casos, los *bots* empleados en los grupos de Telegram podrían estar operando con credenciales institucionales válidas, lo que permitiría realizar consultas directas a sistemas oficiales y extraer datos en tiempo real para su posterior venta.

Se identificó también el uso de otros comandos que permiten acceder a datos personales sin necesidad de conocer el número de DNI de la persona titular; por ejemplo, por medio de su nombre, placa de vehículo o número de celular. En relación con este último mecanismo de consulta, los datos son presentados bajo la etiqueta "OSIPTEL DATABASE – CEL". Es importante destacar que el Organismo Supervisor de Inversión Privada en Telecomunicaciones (OSIPTEL) es la entidad estatal encargada de regular y supervisar los servicios de telecomunicaciones en Perú, incluyendo el registro de líneas móviles asociadas a personas naturales o jurídicas.

Otros comandos identificados en los *bots* fueron **/hogar** y **/ag**, que permiten acceder a redes completas de vínculos familiares. Al ingresar el número de DNI en el comando **/hogar**, el *bot* otorga información del domicilio registrado, el estado económico del hogar, su clasificación socioeconómica ("pobre extremo", "pobre" o "no pobre", de acuerdo con la clasificación del Sistema de Focalización de Hogares – SISFOH, en Perú), precisiones respecto a si se encuentra en zona rural o urbana, así como los datos de cada uno de los integrantes del núcleo familiar: nombres, apellidos, DNI y fecha de nacimiento.

42. El certificado C4 contiene información básica del DNI de una persona. Es un certificado informativo, que no reemplaza al DNI, pero se usa como medida de seguridad para comprobar una identidad en formularios de algunos servicios digitales. Disponible en: **https://www.gob.pe/8803-solicitar-certificado-de-inscripcion-c4**

Finalmente, durante la investigación también se observó la venta de lo que aparentan ser certificados oficiales de antecedentes policiales y judiciales, documentos que, en circunstancias regulares, solo podrían ser emitidos mediante trámites formales (con un precio y tiempo de expedición) ante el Ministerio del Interior (PNP) o el Poder Judicial del Perú. En ambos casos, los *bots* generan archivos en formato PDF, presuntamente emitidos por la Policía Nacional del Perú y por el Poder Judicial nacional, respectivamente. Los documentos incluyen datos como imagen facial, nombres y apellidos completos, firma digital, número de documento, nacionalidad y el resultado sobre si la persona registra condenas o antecedentes (ver Imagen 6).

Imagen 6. Evidencia visual sobre venta de datos con certificados oficiales de antecedentes policiales y judiciales

El acceso inmediato a estos certificados, sin pasar por el proceso oficial de solicitud que normalmente requiere autenticación, pago de una tasa y un tiempo de espera de horas o días, plantea interrogantes sobre su posible origen y sobre eventuales vulneraciones a las plataformas estatales de emisión digital. En algunos casos, los certificados fueron generados en la misma fecha y hora exactas que la consulta realizada al *bot* en Telegram, como se ve en la Imagen 6, lo que abre la pregunta sobre si estos sistemas podrían estar directamente vinculados, de manera no autorizada, con bases de datos oficiales, o si se trata de una simulación técnicamente avanzada de los formatos institucionales.

La coincidencia temporal entre la solicitud y la emisión, junto con la fidelidad de los formatos, puede indicar a la hipótesis de que el acceso no proviene de una base filtrada estática, sino de una interacción directa con los sistemas oficiales. Sin embargo, a falta de evidencias concluyentes, ambos escenarios siguen abiertos y requieren una verificación técnica más profunda.

4.2.1 Contexto tecnopolítico y legal

En Perú, al igual que en los otros países de la región, las filtraciones masivas de datos personales son un fenómeno recurrente que afecta tanto a instituciones públicas como privadas[43]. En junio de 2025, de hecho, la Autoridad Nacional de Protección de Datos Personales (ANPDP) peruana emitió una alerta urgente tras una filtración que expuso 16 mil millones de contraseñas vinculadas a servicios como Apple, Google y Facebook, instando a la ciudadanía a cambiar sus claves de inmediato para reducir el riesgo de fraudes y suplantación de identidad[44].

Este escenario general también se refleja en el uso de aplicaciones de mensajería, donde se han documentado incidentes que evidencian cómo las filtraciones pueden alimentar directamente el mercado ilegal de datos. En 2024, durante la emisión de un reportaje televisivo[45], periodistas fueron amenazados a través de WhatsApp por actores maliciosos quienes les hicieron llegar sus propios datos personales obtenidos desde Telegram. Las amenazas consistieron en el envío de fichas de la RENIEC con datos completos de los periodistas, acompañadas de mensajes intimidatorios. Al exhibir su acceso a esta información personal, los responsables buscaban infundir temor y demostrar su capacidad de rastreo. El mismo reportaje televisivo reveló que los datos de tales periodistas estaban disponibles en grupos de Telegram, como los analizados en esta investigación, en los cuales basta con ingresar un número de documento para acceder a datos personales de cualquier persona[46].

Meses después, aún en 2024, se reportó otro incidente de gran magnitud en Perú: los datos de más de 3 millones de clientes de Interbank fueron robados y publicados en la *dark web*. Según la cobertura periodística del caso[47], un usuario anunció que esos datos podían "conseguirse" vía Telegram, sin que el reporte verificara su comercialización efectiva en dicha plataforma. Más allá del aviso, la cobertura aporta un elemento técnico relevante para el análisis. En los archivos asociados al caso aparece un script que describe un acceso a una base alojada en New Relic (proveedor de Interbank) mediante credenciales (usuario y contraseña), y revela conocimiento de detalles internos de la estructura del servidor al que se intentaba acceder[48]. Estos indicios no constituyen una prueba concluyente de la ruta de exfiltración, pero fortalecen la hipótesis de un acceso con información interna o de

43. Cuzcano, X. (2025). Filtraciones de datos: el costo ciudadano de la negligencia digital. Disponible en: **https://www.derechosdigitales.org/recursos/filtraciones-de-datos-el-costo-ciudadano-de-la-negligencia-digital/**

44. Infobae (2025). Gobierno del Perú lanza alerta urgente por filtración de 16 mil millones de contraseñas: ANPD pide cambiar claves de inmediato. Disponible en: **https://www.infobae.com/peru/2025/06/24/gobierno-del-peru-lanza-alerta-urgente-por-filtracion-de-16-mil-millones-de-contrasenas-anpd-pide-cambiar-claves-de-inmediato/**

45. Disponible en: **https://www.youtube.com/watch?v=9UvS9SBuMVA**

46. Ibid

47. Ojo Público (2024). El negocio ilegal de la información personal: la ruta detrás del robo de datos de Interbank. Disponible en: **https://ojo-publico.com/5390/ciberdelincuencia-la-ruta-detras-del-robo-datos-interbank**

48. Infobae (2024). Caso Interbank: ¿Qué habría detrás de la extorsión y la filtración de datos de clientes por el supuesto 'hacker'? Disponible en: **https://www.infobae.com/peru/2024/10/31/caso-interbank-filtracion-de-datos-de-millones-de-clientes-se-habria-dado-tras-fallidas-negociaciones-con-extorsionador-digital/**

una configuración de seguridad vulnerable, y ayudan a explicar cómo filtraciones de esta escala pueden alimentar, directa o indirectamente, los circuitos ilegales de datos en mensajería y foros.

En términos normativos, el marco de protección de datos vigente en Perú tiene más de una década de existencia. Está definido por la Ley N.° 29733 - Ley de Protección de Datos Personales, promulgada en 2011, cuyo objetivo es garantizar el derecho fundamental a la protección de los datos personales reconocido en la Constitución[49]. La norma considera como datos sensibles aquellos que incluyen información biométrica, ingresos económicos, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical, así como información vinculada a la salud o a la vida sexual; categorías que se corresponden con varios de los tipos de datos identificados como objeto de comercialización en esta investigación.

Entre los principios rectores de la ley se encuentra la seguridad, que obliga a los responsables por actividades de tratamiento a implementar medidas técnicas, organizativas y legales para evitar accesos no autorizados y garantizar la integridad de los datos. Asimismo, la norma reconoce expresamente el derecho de las personas titulares a ser indemnizadas cuando un tratamiento indebido de datos les cause perjuicio.

En noviembre de 2024 se aprobó un nuevo reglamento a la Ley de Protección de Datos Personales[50] en Perú, que introduce avances relevantes como la obligación de notificar incidentes de seguridad a la ANPDP, la exigencia de políticas de seguridad documentadas y la implementación de controles de acceso más estrictos. Aunque estas reformas buscan robustecer la protección a las personas titulares, la ausencia de reglas diferenciadas para agentes públicos de tratamiento de datos sigue siendo una limitación clave de la ley.

Esta falta de especificidad es relevante porque las entidades estatales gestionan grandes volúmenes de datos –incluyendo datos sensibles–, lo que amplifica el impacto potencial de cualquier filtración o uso indebido. Sin criterios más rigurosos de seguridad, transparencia y rendición de cuentas aplicables al sector público, la ley corre el riesgo de ofrecer un nivel de protección desigual, dejando a la ciudadanía más expuesta precisamente frente a quienes concentran los mayores repositorios de datos personales.

La aplicación de la ley está a cargo de la ANPDP, adscrita al Ministerio de Justicia y Derechos Humanos, a través de la Dirección Nacional de Justicia[51]. La ANPDP cuenta con potestad sancionadora y coactiva y, en teoría, con independencia para supervisar tanto a actores públicos como privados. Sin embargo, al estar institucionalmente adscrita al dicho Ministerio, esa autonomía puede resultar limitada en la práctica, especialmente cuando se trata de supervisar a entidades estatales o de imponer sanciones dentro del mismo ámbito gubernamental.

49. Para más información, ver: **https://www.gob.pe/institucion/congreso-de-la-republica/normas-legales/243470-29733**

50. Disponible en: **https://www.gob.pe/institucion/smv/normas-legales/6426760-016-2024-jus**

51. Disponible en: **https://www.gob.pe/institucion/anpd/normas-legales/2018427-29733-2011**

En paralelo, desde 2013 está vigente la Ley Nº 30096 - Ley de Delitos Informáticos[52], que tipifica conductas como el acceso ilícito a sistemas y la interceptación de datos informáticos, estableciendo penas agravadas cuando los hechos involucran información clasificada o afectan la defensa y la seguridad nacional. Reformas recientes, introducidas mediante decretos y convenios interinstitucionales, han fortalecido la coordinación entre la Policía Nacional, el Ministerio Público y organismos especializados, creando unidades de cibercrimen y protocolos de intercambio de información. Asimismo, se incorporaron obligaciones de capacitación técnica para personas funcionarias y autoridades judiciales en materia de investigación digital. Finalmente, en materia de ciberseguridad, Perú elaboró la Estrategia Nacional de Seguridad y Confianza Digital 2021-2026[53], cuyos ejes incluyen la promoción de una cultura de seguridad, la protección de activos críticos, el desarrollo de capacidades y la provisión de servicios digitales. El documento, sin embargo, no fue adoptado formalmente como política de Estado[54]. Tal omisión limita su fuerza normativa y proactiva, y refleja la fragilidad institucional para articular respuestas efectivas en materia de ciberseguridad. Esta falta de implementación también evidencia la desconexión entre las políticas de ciberseguridad y las de protección de datos personales, que en la práctica deberían abordarse de manera conjunta como dimensiones complementarias de la seguridad y la confianza digital.

En los hallazgos de la investigación, esta fragilidad institucional se manifiesta en la amplia circulación de datos personales y de documentos que parecen reproducir el formato o los atributos de los emitidos por entidades públicas. Aunque no es posible determinar con certeza su origen, la similitud con registros oficiales sugiere deficiencias en los controles de seguridad y en la supervisión sobre el tratamiento de datos, incluso de datos sensibles.

52. Disponible en: **https://www.gob.pe/institucion/mpfn/informes-publicaciones/1678028-ley-n-30096**

53. Disponible en: **https://www.gob.pe/7025-presidencia-del-consejo-de-ministros-secretaria-de-gobierno-digital**

54. Derechos Digitales (2025). Ciberseguridad en América Latina: Estrategias nacionales en 2024. Disponible en: **https://www.derechosdigitales.org/wp-content/uploads/DD_CYRILLA_ESP_2024.pdf**

4.3 Argentina

En Argentina se identificaron seis canales y un grupo, con un modelo de operación distinto al observado en Brasil y Perú. En este caso, el esquema prioriza la comunicación directa y discreta entre vendedores y compradores. Se observó que los canales funcionan como punto de entrada: allí se difunden anuncios, planes y evidencias de venta, mientras que las transacciones se concretan de manera personalizada mediante chats uno a uno. El alcance de los espacios investigados es el siguiente:

Tabla 4. Número de suscriptores de canales observados

Canal1	Canal2	Canal3	Canal4	Canal5	Canal6	Grupo1
8.698	3.109	915	539	12.847	2.395	1.280

Como predominan los canales sobre los grupos, se cambia la visibilidad de las figuras administradoras, ya que en los canales de Telegram no es posible acceder a la lista de suscriptores ni identificar quién gestiona el espacio, lo que dificulta comprender cómo se estructuran.

Se identificó que el modelo en Argentina está mucho más centralizado en vendedores humanos. Así, en lugar de permitir búsquedas gratuitas o interacciones autónomas con *bots* desde el grupo, las operaciones se canalizan a través del chat privado entre cliente y vendedor. Una vez iniciado el contacto, el vendedor remite los precios y medios de pago disponibles, y recién tras concretar la transacción, el *bot* es añadido y activado en ese mismo chat privado. Este funcionamiento pudo observarse a partir de las referencias que los propios vendedores publican en los canales abiertos, donde explican el modo de operación y los pasos que deben seguir las personas *interesadas*. La estrategia empleada elimina por completo las búsquedas gratuitas o parciales y se establece como regla que todo el proceso sea pago, bajo una lógica de trato personalizado que simula una "atención directa al cliente".

En esta línea, los vendedores suelen ofrecer distintos "planes" según el tipo y volumen de información requerida. En algunos casos, el modelo incluye accesos temporales, es decir, permisos de uso limitados a un período determinado (como horas o días) durante el cual el comprador puede realizar consultas y, en ciertos casos, descargar los resultados. En otros casos, se comercializan paquetes por volumen de búsquedas, que restringen la cantidad de datos obtenidos en función del valor del pago realizado. El esquema de precios se encuentra más orientado al uso de *tokens* como moneda interna, entendidos como unidades virtuales de pago que se adquieren previamente y luego se consumen dentro del *bot* para habilitar funciones o consultas específicas. Este sistema refuerza un modelo transaccional inmediato, en el que la persona usuaria compra solo lo que necesita.

Se identificaron paquetes que ofrecen acceso desde $3.5 USD por día –con uso del *bot* habilitado solo por 24 horas– hasta servicios «permanentes» por $15 USD, que otorgan acceso continuo sin límite de tiempo. También se encontraron modalidades basadas en *tokens*, como la venta de 1000 unidades por $100 USD, donde cada *token* equivale a una consulta o una función habilitada dentro del *bot*. El método más

utilizado es Mercado Pago, plataforma digital de pagos desarrollada por Mercado Libre. Esta herramienta se ha convertido en una de las más populares de Argentina (y toda América Latina)[55] para transacciones electrónicas.

A diferencia de los sistemas de pago predominantemente utilizados en Brasil o Perú (que funcionan, respectivamente, como mecanismos de pago instantáneo entre personas y billeteras digitales), Mercado Pago opera como intermediario financiero dentro de una plataforma comercial, gestionando cuentas de usuarios y ofreciendo mayor formalidad en las transacciones. Sin embargo, su uso por vendedores en los canales ilícitos sugiere que, pese a su estructura empresarial y trazabilidad potencial, también puede ser aprovechado para operaciones de este tipo. En la práctica, al momento de realizar el pago se visualiza el nombre de la persona o empresa receptora, lo que indica que, al igual que en los casos de los otros países investigados, no se trata de un sistema completamente anónimo, aunque su intermediación introduce un nivel diferente de opacidad operativa.

Sin embargo, algunos espacios analizados también han migrado hacia el uso de criptomonedas, lo cual representa un nivel mayor de encubrimiento transaccional y menor trazabilidad, en línea con prácticas comunes en mercados ilícitos globales[56]. Esta diversidad de medios de pago responde a las restricciones locales, como los controles bancarios y los límites al envío de dinero en efectivo o digital y sugiere la necesidad de los vendedores de evadir la trazabilidad de las transacciones a través del sistema financiero formal.

La presencia de registros de compras anteriores y respuestas automáticas compartidas como "demostración" en canales públicos observados –es decir, ejemplos de consultas reales compartidos por los vendedores para mostrar que el servicio funciona (llamados "referencias")– evidencia que no se trata de transacciones aisladas. Por el contrario, la reiteración de estos ejemplos indica un flujo sostenido de adquisiciones de datos, reflejando la regularidad con que estos mercados digitales están siendo utilizados.

En varios de los ejemplos identificados, los *bots* devuelven resultados que incluyen datos presuntamente obtenidos del Registro Nacional de las Personas (RENAPER), entidad responsable de la base de datos de identidad en Argentina. Esta inferencia se sostiene tanto porque dichos datos (fotografía, número de documento, filiación y otros) solo deberían constar en el RENAPER, como porque algunos de los archivos analizados muestran formatos y marcas que coinciden con los utilizados oficialmente por esta institución. Entre estos elementos está la presencia de un código denominado por los *bots* "IDARG", un identificador alfanumérico incluido en el DNI electrónico argentino y utilizado para validar la autenticidad del documento.

Uno de los comandos más utilizados en los canales argentinos es **/dni**, el cual, dentro de los paquetes de pago ofrecidos por los vendedores, permite acceder a información

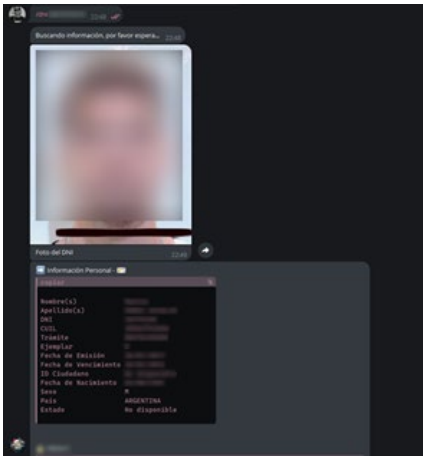
55. Para más información, ver: **https://paymentscmi.com/insights/metodos-pagamento-mais-utilizados-america-latina-brasil-mexico-chile-peru-colombia-argentina/**

56. Infobae (2025). Criptomonedas: el arma financiera de los cárteles. Disponible en: **https://www.infobae.com/mexico/2025/07/20/criptomonedas-el-arma-financiera-de-los-carteles/**

detallada de cualquier persona con solo ingresar su número de documento nacional de identidad. Así como en Perú, la respuesta del *bot* incluye la imagen facial oficial extraída del documento y, en algunos casos, su firma escaneada.

En varios canales estas imágenes comparten un patrón visual: trazos de seguridad y marcas de agua institucionales, es decir, elementos gráficos utilizados habitualmente para autenticar documentos oficiales y prevenir su falsificación, como sellos digitales, fondos tramados o escudos con relieve. Hay casos de fotografías con inscripciones de entidades como colegios y ministerios específicos, lo que sugiere filtraciones de datos que podrían provenir de sistemas internos de esas instituciones escolares y de la administración pública (ver Imagen 7).

Imagen 7. Evidencia visual sobre venta de datos a través del comando **/dni**



Es particularmente alarmante un caso donde se muestra la imagen de una adolescente, junto a datos como nombre, DNI y fecha de nacimiento, con una marca de agua que indica "Sistema Federal de Comunicaciones Policiales" (SIFCOP). Este sistema es una herramienta oficial restringida, utilizada exclusivamente para el intercambio de información de interés criminal entre fuerzas policiales y organismos judiciales[57]. Su acceso está regulado por protocolos estrictos, lo que agrava la potencial filtración ocurrida.

Además de eso, los *bots* entregan una ficha estructurada con datos como nombre completo, número de DNI, CUIL (Código Único de Identificación Laboral), número de trámite, número de ejemplar, fecha de emisión y vencimiento del documento, nacionalidad, sexo, fecha de nacimiento y un estado registral que puede incluir un aviso de fallecimiento.

A esta información se suma la dirección completa de la persona: calle, número, barrio, código postal, ciudad, municipio, provincia e incluso piso o monoblock[58]. En algunos casos, la respuesta incluye un enlace directo a Google Maps que facilita

57. Para más información, ver: **https://www.argentina.gob.ar/seguridad/secretaria-seguridad/subsecretaria-de-investigacion-criminal-y-cooperacion-judicial-4**

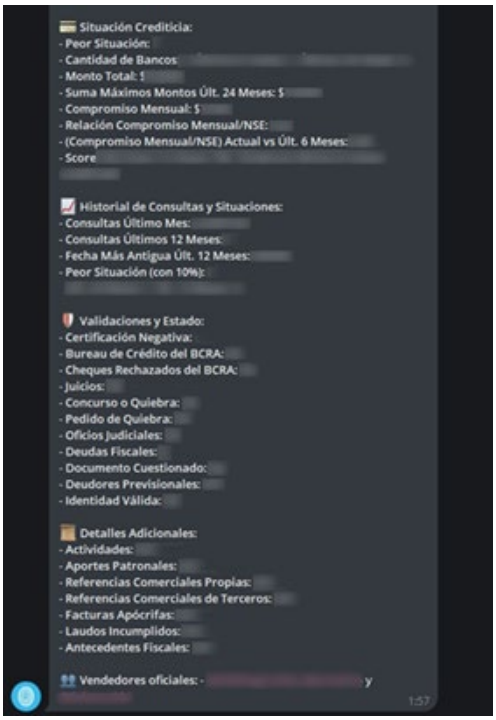
58. Monoblock en Argentina es un bloque de departamentos dentro de un conjunto habitacional, generalmente parte de construcciones estatales o viviendas sociales. Suele identificarse junto al piso y número de unidad para ubicar con precisión un domicilio en complejos edilicios.

la geo ubicación del domicilio, elevando significativamente el riesgo de prácticas como seguimiento, vigilancia privada, acoso o secuestro. También se encuentra tras la consulta información detallada contenida en la licencia de conducir de la persona titular del DNI (como número, categoría y fechas de emisión y vencimiento).

En algunos espacios también es posible acceder a información financiera detallada de personas a través del comando **/nosis** seguido del número de CUIT (Código Único de Identificación Tributaria) o DNI. Este comando parece hacer alusión a la base de datos del sistema crediticio "NOSIS", una de las plataformas más conocidas en Argentina para reportes financieros y de riesgo crediticio[59].

Tras este comando, en primer lugar, el *bot* muestra información personal básica. Luego, el reporte detalla el estado laboral de la persona: si es empleadora, si pertenece a una sociedad, si es empleada o monotributista, y si ha estado bancarizada en los últimos meses. También se indica la antigüedad en la base de datos de la Administración Federal de Ingresos Públicos (AFIP). Adicionalmente, se accede a la situación crediticia de la persona (ver Imagen 8). Se muestra la "peor situación" registrada, la cantidad de bancos involucrados, el monto total adeudado, el compromiso mensual (relación entre ingresos y deuda), el *score* crediticio, y su tendencia a lo largo del tiempo. En otras palabras, esta sección ofrece una radiografía clara del comportamiento financiero de la persona.

Imagen 8. Evidencia visual sobre venta de datos con información de la situación crediticia

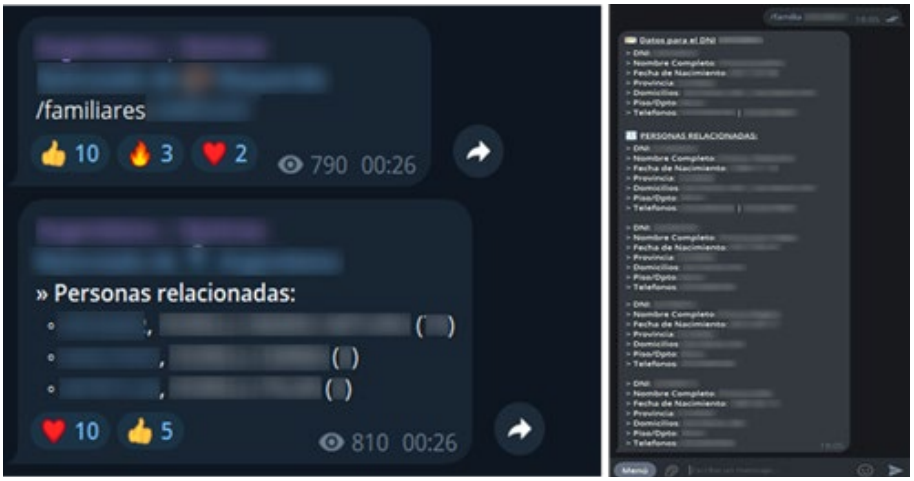


59. "NOSIS fue fundada en 1988 con el objeto de brindar información de antecedentes comerciales, mercados financieros en línea y comercio exterior para aportar herramientas analíticas que faciliten la toma de decisiones. Más de 25.000 clientes han comprobado que nuestras [sus] bases de datos, de fuentes propias y públicas, son las más completas y actualizadas del mercado." Disponible en: **https://www.nosis.com/es/institucional/quienes-somos**

El *bot* también revela campos técnicos del DNI (como el código de barras y líneas completas del sistema de lectura mecánica MRZ), elementos que no solo validan el documento, sino que permiten su clonación o replicación para fines maliciosos. Además, como ya mencionado, uno de los elementos técnicos más alarmantes que devuelve el *bot* es el IDARG, un código alfanumérico presente en el DNI electrónico argentino, utilizado para validar la autenticidad del documento. Su inclusión en estas respuestas indica un acceso a capas profundas del sistema de emisión de identidad del país.

En algunos casos, el uso del mismo comando de consulta ya sea **/dni**, **/consulta** o variantes, 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 el comando **/familia** o **/familiares** seguido del número de DNI, a través de lo cual el *bot* es capaz de devolver tanto los datos de la persona consultada como los de sus familiares directos, como se muestra en la Imagen 9. Las respuestas generadas incluyen información detallada como nombres completos, fechas de nacimiento, domicilio, provincia, y en varios casos también los números telefónicos vinculados a cada persona. En algunos casos, incluso se muestra la edad actual de los familiares.

Imagen 9. Evidencia visual sobre venta de datos a través del comando **/familia**



Otros comandos de búsqueda observados incluyen el nombre, teléfono y patente de 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. Mediante el comando **/empresa** seguido de un número de CUIT, los *bots* devuelven datos detallados sobre una entidad registrada oficialmente en el país.

4.3.1 Contexto tecnopolítico y legal

Así como los otros países de la región, Argentina ha enfrentado un histórico de incidentes graves de seguridad de datos. En 2021, por ejemplo, más de 116 mil fotografías del RENAPER fueron compartidas indebidamente en Telegram. El episodio dio lugar a una investigación judicial y a la apertura de un sumario interno[60], aunque hasta septiembre de 2025 no se han publicado resultados concluyentes sobre su alcance o sobre posibles responsables.

En ese mismo año, otro ataque comprometió la base de datos pública del sistema de licencias de conducir, dejando a más de 6 millones de personas en riesgo[61]. Estos episodios evidencian la fragilidad de los mecanismos de seguridad de bases de datos estatales, y muestran además que el problema es previo y trasciende el uso de Telegram.

Sin embargo, es importante destacar que el país fue pionero en la región en materia regulatoria: en el año 2000 sancionó la Ley N° 25.326 de Protección de Datos Personales[62], una de las primeras de América Latina. La norma "tiene por objeto la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean estos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre".

Establece derechos a las personas titulares de datos como los de acceso, rectificación, supresión, confidencialidad y actualización de los datos, e impone obligaciones de seguridad de la información a quienes los traten. No obstante, la ley no establece un régimen diferenciado para agentes públicos, a pesar de que el Estado es el principal recolector y custodio de datos ciudadanos.

La aplicación de la Ley N° 25.326 recae en la Agencia de Acceso a la Información Pública (AAIP), autoridad creada en 2016[63], que es dependiente de la Jefatura de Gabinete de ministros. Según el artículo 29 de la Ley de Protección de Datos, entre las funciones de la Agencia se encuentran controlar la observancia de las normas de seguridad de datos y aplicar sanciones administrativas en caso de incumplimiento. Sin embargo, al estar inserta bajo la estructura del propio Poder Ejecutivo, su capacidad para fiscalizar vulneraciones provenientes de organismos estatales puede resultar limitada.

En 2008 Argentina reforzó su cuadro penal con la sanción de la Ley N° 26.388, que modificó el Código Penal e incorporó delitos informáticos al capítulo de "Violación

60. Infobae (2024). Volvieron a publicar más de 116 mil fotos y números de DNI y pasaporte de argentinos robados al Renaper. Disponible en: **https://www.infobae.com/politica/2024/04/03/volvieron-a-publicar-mas-de-116-mil-fotos-y-numeros-de-dni-y-pasaporte-de-argentinos-robados-al-renaper/**

61. Voces Críticas (2024). Robaron del RENAPER 116 mil fotos de ciudadanos argentinos para venderlas por Telegram. Disponible en: **https://www.vocescriticas.com/noticias/2024/04/03/156677-robaron-del-renaper-116-mil-fotos-de-ciudadanos-argentinos-para-venderlas-por-telegram**

62. Disponible en: **https://www.argentina.gob.ar/normativa/nacional/ley-25326-64790**

63. Disponible en: **https://www.argentina.gob.ar/normativa/nacional/ley-27275-265949**

de Secretos y de la Privacidad"[64]. Entre ellos, el artículo 153 bis sanciona con prisión de quince días a seis meses el acceso ilegítimo a sistemas o datos informáticos de acceso restringido, y agrava la pena cuando se trata de datos de organismos públicos o proveedores de servicios financieros. Asimismo, el artículo 157 bis penaliza con prisión de uno a dos años el acceso indebido a bancos de datos personales.

En el ámbito de la ciberseguridad, en septiembre de 2023, Argentina aprobó su Segunda Estrategia Nacional de Ciberseguridad[65], un documento que, a primera vista, representó un avance significativo en la región. La estrategia incluyó entre sus objetivos y lineamientos principios de derechos humanos, perspectiva de género, protección de sectores en situación de vulnerabilidad, cooperación internacional, soberanía digital y resguardo de infraestructuras críticas. También contempló objetivos como el fortalecimiento institucional, la protección de sistemas del sector público, la concientización ciudadana y el desarrollo de un marco normativo acorde a los nuevos desafíos tecnológicos.

Sin embargo, estos avances quedaron en entredicho tras una serie de reformas recientes en la gobernanza de la ciberseguridad[66]. En julio de 2024, la reestructuración del Sistema de Inteligencia Nacional disolvió la Agencia Federal de Inteligencia y restituyó funciones a la vieja Secretaría de Inteligencia del Estado (SIDE), así como la AAIP, bajo control directo del Poder Ejecutivo[67]. El año siguiente, mediante el Decreto 274/2025, la SIDE asumió el control de la Agencia Federal de Ciberseguridad, la implementación de la Estrategia Nacional y la operación del **CERT.ar**[68]. Poco después, en mayo de 2025, la SIDE aprobó el Plan de Inteligencia Nacional (PIN), declarado "secreto", al que solo tienen acceso el presidente, la SIDE y una comisión bicameral[69]. Según filtraciones de prensa, este plan otorga facultades para recabar información sobre personas que, a criterio del gobierno, "erosionen" la confianza pública en sus políticas[70], lo que profundiza la preocupación por la falta de transparencia y control democrático.

64. Disponible en: **https://www.argentina.gob.ar/normativa/nacional/ley-26388-141790/texto**

65. Disponible en: **https://www.boletinoficial.gob.ar/detalleAviso/primera/293377/20230904**

66. Mantilla-León, L. y Meira, M. (2025). Cuando la ciberseguridad es cooptada por la inteligencia estatal. Disponible en: **https://www.derechosdigitales.org/recursos/cuando-la-ciberseguridad-es-cooptada-por-la-inteligencia-estatal/**

67. DEF (2024). Dentro de la SIDE, así será la Agencia Federal de Ciberseguridad. Disponible en: **https://defonline.com.ar/seguridad/dentro-de-la-side-asi-sera-la-agencia-federal-de-ciberseguridad/**

68. Disponible en: **https://www.boletinoficial.gob.ar/detalleAviso/primera/5870460/20250416?suplemento=1**

69. Para más información, ver: **https://www.argentina.gob.ar/noticias/comunicado-oficial-numero-101**

70. La Nación (2025). El Gobierno niega que la SIDE haga espionaje interno, pero el Congreso revisa el Plan de Inteligencia. Disponible en: **https://www.lanacion.com.ar/politica/el-gobierno-niega-que-la-side-investigue-a-opositores-o-quienes-manipulen-la-opinion-publica-nid25052025/**

En este contexto, disponer la política de ciberseguridad bajo una estructura de inteligencia estatal cerrada y sin controles democráticos implica que la estrategia nacional pierde independencia y capacidad de aplicación efectiva. En lugar de garantizar la protección de las personas y de las infraestructuras críticas, como establecen los objetivos formales de la Estrategia argentina, la falta de autonomía limita seriamente su capacidad de respuesta frente a vulneraciones como las documentadas en esta investigación, que apuntan a un posible aprovechamiento indebido de información proveniente de bases públicas y su posterior circulación en Telegram.

VOLVER AL ÍNDICE

5 TENDENCIAS REGIONALES

Esta sección destaca tres tendencias transversales a los hallazgos nacionales de la investigación, relacionándolas con características propias de América Latina como región. La primera apunta a la posible procedencia de una parte significativa de los datos que circulan en grupos y canales de Telegram desde bases de datos públicas. Si bien no es posible confirmarlo de manera concluyente, diversos indicios (como formatos, codificaciones y referencias institucionales) sugieren que parte de la información podría haber sido obtenida mediante *scraping*, filtraciones o uso indebido de credenciales. Este escenario revelaría no solo limitaciones en la aplicación de las normas de protección de datos, sino también debilidades en la seguridad de los sistemas que almacenan y gestionan la información personal, en un contexto de avance acelerado de políticas de digitalización del Estado en países latinoamericanos. La segunda tendencia se vincula con el género y muestra cómo el mercado ilegal de datos opera como insumo de la violencia de género facilitada por tecnologías, potenciando el control, la extorsión y el silenciamiento de mujeres y personas LGBTQIA+. Finalmente, la tercera subraya la especial vulnerabilidad de niñas, niños y adolescentes (NNA), agravada por prácticas que los y las infantilizan e hipersexualizan con relación al mercado ilegal de sus datos.

5.1 Indicios de origen público de los datos y fragilidades en la gestión de la información

Si bien no es posible determinar con certeza el origen de los datos que se comercializan en los grupos y canales analizados, distintos indicios apuntan a que una parte significativa de la información podría haber sido obtenida a partir de bases de datos públicas o registros oficiales. La coincidencia en el formato de los campos, la terminología empleada y la estructura de los archivos sugiere la posible existencia de filtraciones, accesos indebidos o usos no autorizados de información estatal, lo que plantea serios desafíos en materia de seguridad de la información y gobernanza de datos, sobre todo considerando las políticas de digitalización del Estado y de servicios públicos que están siendo acrecentadas en América Latina.

Uno de los indicios más importantes sobre el posible origen de los datos comercializados ilegalmente se podría encontrar en los propios espacios donde se promueve el uso de *bots*. En algunos canales, especialmente en Argentina, los administradores reconocen explícitamente que los datos provienen de técnicas de *scraping* –una técnica automatizada que permite extraer grandes volúmenes de datos de sitios web– lo que permite inferir que la información recolectada incluiría datos de bases oficiales, a partir de la naturaleza de los registros y de la presencia de marcas de agua y formatos estales. El término *scrap* aparece mencionado en mensajes difun-

didos dentro de los canales como una habilidad técnica clave para acceder, recolectar y posteriormente comercializar información personal de gran escala. En este contexto, se trataría de un proceso mediante el cual se recolecta sistemáticamente información personal desde bases de datos.

Además, en algunas de las evidencias visuales analizadas, se presentan estructuras de datos en formato JSON, un estándar ampliamente utilizado para el intercambio de información entre sistemas porque organiza los datos en pares de "clave:valor". La identificación de este formato permite inferir que la información pudo haber sido extraída y procesada directamente desde bases de datos o sistemas automatizados, ya que su estructura uniforme y masiva es típica de entornos digitales y no de compilaciones manuales. También se menciona que el *bot* se actualiza con regularidad, lo que requiere un mecanismo de alimentación constante que difícilmente puede mantenerse manualmente.

Otro factor es que en el caso de los tres países analizados, se identificaron datos cuya naturaleza y nivel de detalle coinciden con aquellos que, en principio, solo deberían encontrarse en bases de datos públicas o en registros administrativos del Estado. El histórico vacunal o de beneficios sociales en Brasil, los certificados de antecedentes policiales y judiciales peruanos y los registros del RENAPER argentino con el código IDARG son algunos de los ejemplos más relevantes.

La presencia de esta información en entornos de compraventa y automatización en Telegram podría reflejar fallas estructurales en las arquitecturas legales e institucionales de protección de datos y ciberseguridad en América Latina. Como fue señalado, este fenómeno ocurre en un contexto de digitalización acelerada de las políticas y servicios públicos en la región, impulsada por estrategias estatales impulsadas bajo el argumento de la eficiencia[71]. Sin embargo, este proceso no ha estado acompañado por estándares equivalentes de seguridad, transparencia y rendición de cuentas, incluso en relación con el tratamiento de datos personales que involucra. La expansión de infraestructuras tecnológicas sin una gobernanza sólida ha traído consigo riesgos crecientes de exposición, filtración o reutilización indebida de información estatal. Como fue mencionado anteriormente, si bien no es posible establecer una relación directa, en los casos de Argentina, Brasil y Perú se identifican indicios que apuntan a vulnerabilidades vinculadas con estos procesos.

En este sentido, la venta de datos personales en Telegram podría estar vinculada a una debilidad en las arquitecturas legales e institucionales de protección de datos y ciberseguridad en América Latina. El ecosistema de extracción automatizada e ilegítima de datos, que ocurre en directa contravención a las normativas de protección de datos vigentes en los países analizados, convierte a la identidad de las personas en un insumo comercializable. Como se encontró en la investigación, con un solo comando, es posible acceder a información que va desde el rostro y dirección exacta hasta datos de salud, financieros o vínculos familiares.

Dicha debilidad regional tiene al menos tres dimensiones que requieren de mayor investigación para establecer sus orígenes, causas y respuestas. La primera es nor-

71. Para más información, ver: **https://ia.derechosdigitales.org/wp-content/uploads/2025/02/2024-LATAM-IA_en_el-Estado-ES.pdf**

mativa. Aunque la mayoría de los países de la región cuentan con leyes de protección de datos y con legislaciones de ciberdelitos, éstas no necesariamente resultan suficientes para el contexto de creciente digitalización, sobre todo de los gobiernos. Las leyes de protección de datos rara vez establecen regímenes diferenciados para el sector público, a pesar de que los Estados son los principales recolectores y custodios de información ciudadana.

En paralelo, las legislaciones de ciberdelitos ofrecen herramientas penales donde su aplicación es limitada frente a la magnitud de las filtraciones y la sofisticación de las redes criminales. Además, en el contexto latinoamericano, donde los sistemas de justicia penal enfrentan serias deficiencias estructurales (como la sobrecarga y la selectividad en la persecución) el recurso al derecho penal resulta insuficiente y con bajo potencial didáctico o resocializador, y potencialmente problemático como respuesta principal a los incidentes digitales. Si bien la sanción de los delitos informáticos tiene un valor social de reprobación de este tipo de conducta, centrar la política institucional exclusiva o primordialmente en la vía punitiva deja de lado dimensiones clave como la prevención, la educación digital, la reparación y el fortalecimiento de capacidades institucionales.

Incluso las estrategias nacionales de ciberseguridad tienden a ser de corto alcance y en general presentan serias dificultades para traducirse en políticas públicas efectivas. Como hemos señalado en investigaciones recientes[72], la mayoría de las estrategias en América Latina no incorporan indicadores de cumplimiento ni enfoques de derechos humanos y de género, lo que reduce significativamente su impacto en la protección de la ciudadanía en el entorno digital.

La segunda dimensión de la debilidad es institucional, relacionada a la capacidad de aplicación de las leyes. Las autoridades de protección de datos y los órganos de ciberseguridad suelen carecer de independencia y/o recursos financieros y humanos. En muchos casos forman parte de la misma estructura estatal que deberían supervisar, lo que dificulta investigar filtraciones y sancionar vulneraciones cometidas por entidades públicas. En Brasil, la ANPD recientemente alcanzó una autonomía formal total, pero sigue con recursos limitados; en Perú, la autoridad depende directamente del Ministerio de Justicia y solo recientemente reforzó su reglamento con obligaciones de notificación y medidas de seguridad; y en Argentina, la agencia de protección de datos responde a la Jefatura de Gabinete, mientras que la política de ciberseguridad fue absorbida por el sistema de inteligencia, reforzando la opacidad y eliminando controles externos.

La existencia de autoridades verdaderamente independientes es un elemento central para garantizar la protección efectiva de los datos personales y la seguridad digital. Diversos organismos internacionales, entre ellos la Organización para la Cooperación y el Desarrollo Económico (OCDE)[73], destacan que la autonomía funcional, técnica y financiera de estas entidades es condición indispensable para asegurar la rendición

72. Derechos Digitales (2025). Ciberseguridad en América Latina: Estrategias nacionales en 2024. Disponible en: **https://www.derechosdigitales.org/wp-content/uploads/DD_CYRILLA_ESP_2024.pdf**

73. OCDE (2016). Governance of Regulators' Practices: Accountability, Transparency and Co-ordination. París: OCDE Publishing. Disponible en: **https://www.oecd.org/en/publications/governance-of-regulators-practices_9789264255388-en.html**

de cuentas, sobre todo del Estado en el manejo de información ciudadana. En el contexto de esta investigación, la falta de independencia institucional se traduce en una potencial imposibilidad práctica de esclarecer el origen de los datos que circulan en Telegram o de determinar eventuales responsabilidades públicas frente a filtraciones. Sin capacidad de fiscalización ni recursos suficientes, las autoridades quedan relegadas a un rol reactivo, lo que perpetúa un escenario de vulnerabilidad sistémica en la gestión de la información estatal y de baja aplicación de los marcos normativos vigentes.

Finalmente, la tercera dimensión de la debilidad se vincula con la seguridad de la información en los propios órganos estatales. Si bien las leyes de protección de datos de Argentina, Brasil y Perú reconocen la importancia de contar con medidas de seguridad adecuadas y las estrategias nacionales de ciberseguridad incluyen la protección de infraestructuras críticas y bases de datos públicas como una prioridad, la evidencia relevada sugiere una brecha significativa entre el marco normativo y su implementación práctica. En la mayoría de los casos, las instituciones que concentran y administran grandes volúmenes de información personal carecen de políticas integrales de gestión de riesgos, auditorías técnicas regulares o mecanismos independientes de supervisión.

Esta distancia entre norma y práctica genera vulnerabilidades que, aunque no siempre derivan en filtraciones verificables, amplían las superficies de exposición y los riesgos de accesos indebidos, reutilización o pérdida de información sensible. Además, los altos e históricos índices de filtraciones de datos en la región[74] refuerzan la idea de que América Latina carece de una cultura sólida de seguridad de la información, donde las medidas suelen ser reactivas o fragmentarias. En un contexto de creciente interconexión entre sistemas estatales, la ausencia de gobernanza tecnológica efectiva debilita la capacidad de los Estados para resguardar la integridad de los datos que gestionan y, al mismo tiempo, erosiona la confianza ciudadana en los procesos de digitalización pública.

La facilidad con que operan los grupos y canales de compraventa de datos en Telegram, junto con los posibles usos extorsivos o de suplantación de identidad que se desprenden de estas prácticas, evidencia la magnitud de los riesgos asociados a la gestión deficiente de la información personal. Cuando los datos expuestos presentan características compatibles con registros administrados por entidades oficiales, el problema trasciende la esfera individual y compromete la seguridad colectiva y la confianza en las instituciones públicas. En conjunto, los hallazgos de esta investigación muestran que, pese a los avances normativos en materia de protección de datos y ciberseguridad, la región aún enfrenta un déficit estructural en la capacidad de traducir las normas en garantías efectivas, lo que mantiene abiertos espacios de vulnerabilidad para la ciudadanía.

74. Cuzcano, X. (2025). Filtraciones de datos: el costo ciudadano de la negligencia digital. Disponible en: **https://www.derechosdigitales.org/recursos/filtraciones-de-datos-el-costo-ciudadano-de-la-negligencia-digital/**

5.2 El mercado ilegal de datos personales como insumo para la violencia de género facilitada por las tecnologías

América Latina es una de las regiones más desiguales del mundo, siendo la desigualdad de género una de sus dimensiones más persistentes. Las niñas y mujeres enfrentan niveles alarmantes de violencia estructural[75]. Según la Comisión Económica para América Latina y el Caribe (CEPAL), al menos 4.050 mujeres fueron víctimas de feminicidio en 2022 en América Latina y el Caribe, lo que equivale a una muerte violenta de una mujer por razón de género cada dos horas[76]. A su vez, el Mecanismo de Seguimiento de la Convención de Belém do Pará (MESECVI), de la Organización de los Estados Americanos (OEA), reporta que entre 2018 y 2022 se registraron más de 802.000 casos de delitos sexuales contra mujeres, siendo cerca de 488.000 de las víctimas niñas con menos de 18 años[77].

La población LGBTQIA+, a su vez, enfrenta vulneraciones a sus derechos y su seguridad como consecuencia de los profundos índices de desigualdad estructural basada en género de la región. Brasil, por ejemplo, encabeza desde hace años los registros mundiales de asesinatos a personas trans y travestis. En 2024, se documentaron al menos 291 muertes de personas de la comunidad LGBTQIA+, lo que representa un aumento del 13,2% en relación con el año anterior[78]. Estas cifras reflejan la gravedad de una violencia de género arraigada y persistente, que encuentra en el espacio digital un nuevo terreno de reproducción y amplificación.

En este marco, la violencia de género facilitada por tecnologías (VGFT), definida como "cualquier acto de violencia cometido, asistido o agravado parcial o totalmente mediante tecnologías de información y comunicación contra una persona por razón de su género" (UNFPA)[79], debe entenderse como una continuidad de la violencia fuera de línea hacia los entornos digitales. La VGFT comprende diversas conductas, entre ellas la difusión no consensuada de imágenes íntimas, el acoso cibernético, la manipulación de datos personales para extorsión, y el control coercitivo a través de dispositivos y plataformas[80]. Más que un listado cerrado, la VGFT debe entenderse como un fenómeno en constante evolución marcado por la interacción socio-técnica: no solo avanza la tecnología sino también las formas en que ésta es utilizada para ejercer violencia.

75. Para más información, ver: **https://www.cepal.org/es/tipo-de-publicacion/notas-poblacion**

76. CEPAL (2023). En 2022, al menos 4.050 mujeres fueron víctimas de femicidio o feminicidio en América Latina y el Caribe: CEPAL. Disponible en: **https://www.cepal.org/es/comunicados/2022-al-menos-4050-mujeres-fueron-victimas-femicidio-o-feminicidio-america-latina-caribe**

77. Para más información, ver: **https://belemdopara.org/datosyestadisticas/**

78. g1 (2025). Cresce número de mortes violentas de pessoas LGBTQIAPN+ no Brasil, aponta levantamento. Disponible en: **https://g1.globo.com/ba/bahia/noticia/2025/01/18/mortes-lgbtqiapn-brasil.ghtml**

79. UNFPA (2023). What is technology-facilitated gender-based violence? Disponible en: **https://www.unfpa.org/resources/brochure-what-technology-facilitated-gender-based-violence**

80. Para una tipología de conductas que configuran violencia de género facilitada por tecnologías y sus definiciones, consultar: Report of the Special Rapporteur on Violence against Women, Its Causes and Consequences on online violence against women and girls from a human rights perspective (2018). Disponible en: **https://digitallibrary.un.org/record/1641160?v=pdf**; y Luchadoras y SocialTic. Take back the tech! (2018). Disponible en: **https://www.takebackthetech.net/**

Además de la observación de los grupos y canales de compraventa de datos en Telegram, esta investigación incluyó la búsqueda documental de publicaciones y testimonios públicos en redes sociales que hicieran referencia a estas dinámicas. En ese ejercicio, se identificaron denuncias concretas de personas que reportaron haber sido víctimas de distintos tipos de violencia tras la posible adquisición o difusión de sus datos personales a través de esta plataforma. Estos casos permiten observar cómo la comercialización ilegal de información puede vincularse con prácticas de intimidación, acoso y coerción, especialmente dirigidas contra mujeres y personas LGBTQIA+.

En Brasil, por ejemplo, una usuaria denunció en sus redes sociales que un agresor habría adquirido datos suyos y de su madre en un grupo de Telegram y los utilizó para extorsionarla sexualmente, exigiendo videos íntimos bajo amenazas explícitas. De manera similar, en Argentina se documentó un caso en que la fotografía del DNI de una mujer fue compartida en un grupo con comentarios misóginos y homofóbicos, con fines de *doxxeo* y acoso. En Perú, una joven relató haber recibido mensajes intimidatorios con imágenes de armas y amenazas contra su familia, acompañados de la filtración de su documento de identidad, en aparente represalia por haberse pronunciado contra un caso de violencia de género.

Estos casos, identificados durante el mismo periodo de análisis de los grupos y canales observados, ilustran algunos de los posibles usos y finalidades de la compraventa de datos personales. La disponibilidad de información personal amplifica el alcance y la gravedad de la violencia facilitada por las tecnologías, transformando el acceso ilícito a datos en un insumo que facilita prácticas de chantaje, control y hostigamiento. En este sentido, más que incidentes aislados, estos episodios reflejan los riesgos estructurales de un ecosistema donde la falta de seguridad y rendición de cuentas en el manejo de datos permite que la violencia de género encuentre nuevas herramientas y formatos.

Asimismo, en algunos de los grupos peruanos analizados se observaron jerarquías funcionales y dinámicas de interacción marcadas por expresiones abiertamente homofóbicas y misóginas —como "Gato Gay"—, lo que evidencia cómo los espacios digitales donde circulan datos personales también reproducen y refuerzan lógicas de dominación y exclusión basadas en el género y la orientación sexual. Aunque estas manifestaciones no derivan directamente de la compraventa de información, revelan el entorno sociotécnico en el que esta opera: un ecosistema atravesado por discursos violentos y estructuras de poder basadas en el género que legitiman la exposición y el control sobre las identidades disidentes.

Las consecuencias de este tipo de violencia son profundas, impactando tanto a la esfera individual como social. Afectan la salud mental, la seguridad personal y familiar, las oportunidades profesionales y la participación política y social de las víctimas/sobrevivientes[81]. En muchos casos, llevan a la autoexclusión de los espacios digitales, restringiendo el ejercicio de sus derechos a la libertad de ex-

81. Pollicy. (2020). Fighting Violence Against Women Online: A comparative analysis on legal frameworks in Ethiopia, Kenya, Senegal, South Africa and Uganda. **https://ogbv.pollicy.org/legal_analysis.pdf**

presión y de asociación[82] y generando efectos negativos para el debate público, esencial en las sociedades democráticas.

El derecho internacional y regional de los derechos humanos reconoce la VGFT como violencia de género y por tanto, como una violación de derechos humanos. La Relatoría Especial de la ONU sobre la Violencia contra la Mujer[83], reportes del Consejo de Derechos Humanos[84] y el Comité de la Convención sobre la Eliminación de Todas las Formas de Discriminación contra la Mujer (CEDAW, en inglés)[85] han reconocido que las tecnologías digitales pueden ser utilizadas para reproducir y amplificar las violencias basadas en género y advertido sobre la necesidad de generar políticas integrales que reconozcan la continuidad entre lo *online* y lo *offline*. En el ámbito interamericano, la Convención de Belém do Pará obliga a los Estados a prevenir, sancionar y erradicar todas las formas de violencia de género, incluidas las facilitadas por las tecnologías[86].

Pese a los avances en el plano internacional y regional, los marcos jurídicos nacionales en materia de VGFT aún no logran garantizar una protección efectiva a mujeres y personas LGBTQIA+. En general, las respuestas de los Estados han estado más centradas en la dimensión penal que en medidas integrales de prevención, reparación y acompañamiento a las víctimas.

En Brasil, por ejemplo, la situación normativa es bastante fragmentada. A pesar de contar con normas relevantes como la mencionada reforma al Código Penal de 2012 (también llamada Lei Carolina Dieckmann)[87], que tipifica delitos informáticos, y establece leyes que criminalizan conductas como el *stalking*[88] y la violencia política de género[89]; la Ley Fundacional contra la Violencia de Género, Ley 11.340/2006 (llamada Lei Maria da Penha) no contempla de forma expresa a la violencia facilitada por las tecnologías. En consecuencia, el país carece de un marco específico sobre VGFT que garantice a las víctimas de este tipo de violencia el acceso a las medidas de protección y de reparación civil previstas en la Lei Maria da Penha[90].

82. Moolman, J. (2022). Freedom of Expression and Participation in Digital Spaces. UN Women. **https://www.unwomen.org/sites/default/files/2022-12/EP.14_Jan%20Moolman.pdf**

83. Disponible en: **https://digitallibrary.un.org/record/1641160?v=pdf**

84. Para más información, ver: **https://www.unwomen.org/en/digital-library/publications/2022/08/intensification-of-efforts-to-eliminate-all-forms-of-violence-against-women-report-of-the-secretary-general-2022**

85. Para más información, ver: **https://www.acnur.org/fileadmin/Documentos/BDL/2017/11405.pdf**

86. Para más información, ver: **https://belemdopara.org/cim_mesecvi/gender-based-digital-violence-against-women/**

87. Disponible en: **https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm**

88. Disponible en: **https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14132.htm**

89. Disponible en: **https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14192.htm**

90. Disponible en: **https://internetlab.org.br/wp-content/uploads/2025/08/MisoginiaNaInternet.pdf**

En Perú, la Ley 30364, de 2015[91] y el Decreto Legislativo 1410, de 2018[92], tipificaron modalidades de acoso, chantaje sexual y difusión de imágenes íntimas, incluyendo cuando son cometidas mediante tecnologías. Sin embargo, persisten vacíos importantes: la definición de violencia digital sigue siendo difusa, la norma no incluye de manera explícita a mujeres trans ni a la población LGBTIQA+, y su enfoque criminal hace que muchas víctimas no se sientan efectivamente protegidas ni reparadas[93].

Por último, en Argentina, la ya referida reforma penal de 2008[94] incorporó ciberdelitos en línea con el Convenio de Budapest, pero sin perspectiva de género, lo que dejó fuera conductas frecuentes de VG FT como la difusión no consentida de imágenes íntimas[95]. Solo recientemente, en 2023, con la reforma de la Ley 26.485 a través de la llamada Ley Olimpia Argentina[96], se reconoció la violencia digital como una categoría específica de violencia de género y se establecieron mecanismos ágiles para hacer frente, marcando un avance significativo[97] aunque su efectividad dependerá de una implementación adecuada y deberá ser objeto de seguimiento y evaluación en los próximos años.

91. Disponible en: **https://www.defensoria.gob.pe/deunavezportodas/wp-content/uploads/2019/02/Ley3036_erradicarviolencia.pdf**

92. Disponible en: **https://busquedas.elperuano.pe/dispositivo/NL/1690482-3**

93. Hiperderecho (2020). Después de la Ley. Disponible en: **https://hiperderecho.org/wp-content/uploads/2020/12/Informe-2_Despue%CC%81s-de-la-ley.pdf**

94. Disponible en: **https://www.argentina.gob.ar/justicia/derechofacil/leysimple/delitos-informaticos**

95. Ananías Soto, C., Calderón, S., Mow, W., Contreras, A. Giorgelli, M.J., Quiroz, E. (2025). Legislación de la violencia de género facilitada por tecnologías: situación, avances y desafíos pendientes en Latinoamérica. Revista Latinoamericana de Economía y Sociedad Digital, 5, p. 16-46. Disponible en: **https://revistalatam.digital/article/i5-07/**

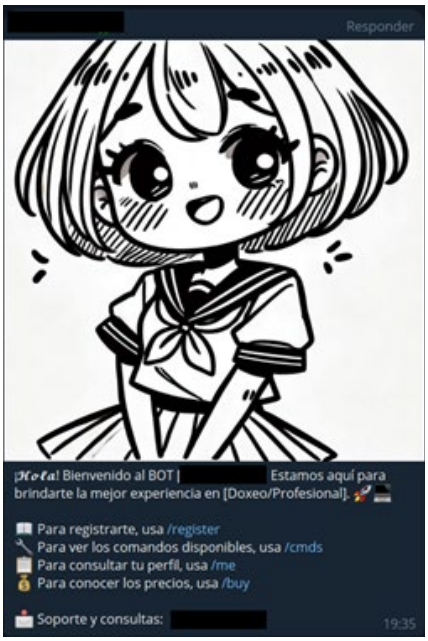
96. Disponible en: **https://www.boletinoficial.gob.ar/detalleAviso/primera/296572/20231023**

97. Ananías Soto, C., Calderón, S., Mow, W., Contreras, A. Giorgelli, M.J., Quiroz, E. (2025). Legislación de la violencia de género facilitada por tecnologías: situación, avances y desafíos pendientes en Latinoamérica. Revista Latinoamericana de Economía y Sociedad Digital, 5, p. 16-46. Disponible en: **https://revistalatam.digital/article/i5-07/**

5.3 Riesgos a las infancias en línea

Un hallazgo alarmante en los entornos analizados es el uso recurrente de ilustraciones de estilo anime, que representan a niñas con apariencia escolar, uniforme y rasgos visuales propios de ese imaginario, como recurso gráfico para dar la bienvenida o promocionar los servicios de los grupos de Telegram, como se ve en los ejemplos abajo (ver Imagen 10):

Imagen 10. Ilustraciones estilo anime usadas para dar la bienvenida o promocionar los servicios de grupos de venta de datos en Telegram



Este no es un fenómeno aislado ni inocente: replica una lógica más amplia de publicidad en América Latina, donde la imagen de mujeres infantilizadas o hipersexualizadas funciona como anzuelo para captar atención y convertirla en clics y compras[98].

Este hallazgo subraya que, más allá de lo técnico o legal, estos ecosistemas requieren una lectura crítica-cultural, donde el diseño y la comunicación visual juegan un rol central en la normalización de prácticas ilícitas.

Además, el uso de este tipo de imágenes se vincula con un contexto más amplio de violencia sexual y objetivación de niñas y adolescentes en América Latina. La región presenta algunas de las tasas más altas de abuso y explotación sexual infantil del mundo, lo que se refleja en fenómenos como el embarazo adolescente y las uniones tempranas.

En Brasil, por ejemplo, el Anuário Brasileiro de Segurança Pública 2025 reporta que 76,8% de todos los casos de violencia sexual registrados en 2024 fueron *"estupro de vulnerável"* (víctimas con menos de 14 años), con predominio de hechos intrafamilia-

98. La Izquierda Diario (2015). Cosificación 2.0: el cuerpo femenino como reclamo de ventas. Disponible en: **https://www.laizquierdadiario.cl/Cosificacion-2-0-el-cuerpo-femenino-como-reclamo-de-ventas**

res[99]. En Perú, según el Ministerio de la Mujer y Poblaciones Vulnerables, de enero a septiembre de 2024 los Centros Emergencia Mujer (CEM) atendieron más de 46 mil casos de niñas, niños y adolescentes víctimas de distintos tipos de violencia. De esta cifra, 16.447 (35,67%) correspondieron a violencia sexual, lo que equivale a aproximadamente 54 personas con menos de 18 años violentadas sexualmente por día[100].

Aunque son datos nacionales, permiten ilustrar un patrón regional de alta victimización infantil, que también se refleja en Telegram, a través del uso de estéticas visuales de hipersexualizadas e infantilizadas de mujeres presuntamente empleadas como estrategias de captación en los grupos.

En línea con el uso problemático de imágenes infantiles, conforme ha sido desarrollado en apartados anteriores, se identificaron en la investigación casos de ventas de datos personales de niñas, niños y adolescentes, así como de datos sobre parentesco y filiación. Dado que esta población se encuentra en desarrollo físico, psíquico, emocional y social, la exposición de sus datos incrementa su vulnerabilidad tanto en línea como fuera de ella, frente a violencias como el acoso y la extorsión. Además, cuando en esas bases se incluyen datos familiares o de las personas cuidadoras (como direcciones, teléfonos o vínculos de parentesco), el riesgo se amplía también hacia las personas adultas responsables, que pueden temer represalias o intentos de coacción dirigidos a ellas o a sus hijas e hijos.

En atención a la especial vulnerabilidad de NNA, la Convención sobre los Derechos del Niño de la ONU establece la doctrina de la protección integral, la que reconoce a esas personas como sujetos de derechos y les garantiza medidas especiales de protección. La Observación General Nº 25 del Comité de los Derechos del Niño[101] órgano de expertos independientes de la ONU reconoce explícitamente que esta protección se extiende a los entornos digitales. Entre otras medidas, la Observación ordena a los Estados revisar y actualizar su legislación para que el entorno digital sea compatible con los derechos de las infancias; integrar la protección en línea en las políticas de niñez; exigir privacidad por diseño, protección de datos y ciberseguridad robustas en productos y servicios usados por NNA; y garantizar remedios rápidos y sensibles a la edad. Asimismo, el texto legal detalla principios de minimización de datos, consentimiento informado (propio o de personas cuidadoras según edad y capacidades), y derechos de acceso, rectificación y supresión relacionados a datos. Atendiendo a lo referido, preocupa como estos principios claramente no son observados en los contextos analizados en la investigación.

En lo que respecta a las legislaciones nacionales de Brasil, Perú y Argentina, el panorama refleja avances importantes (aunque desiguales) para la protección de NNA en entornos digitales, en consonancia con la perspectiva del derecho inter-

99. Para más información, ver: **https://forumseguranca.org.br/wp-content/uploads/2025/07/anuario-2025.pdf**

100. Defensoría del Pueblo (2024). se registran más de 46 000 denuncias de violencia contra niñas, niños y adolescentes. Disponible en: **https://www.defensoria.gob.pe/defensoria-del-pueblo-se-registran-mas-de-46-000-denuncias-de-violencia-contra-ninas-ninos-y-adolescentes/**

101. OHCHR (2021). Observación General núm. 25 (2021) relativa a los derechos de los niños en relación con el entorno digital. Disponible en: **https://www.ohchr.org/es/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation**

nacional. En Brasil, la Constitución Federal[102] consagra la prioridad absoluta en la promoción y protección de derechos de NNA y jóvenes, lo que se operacionaliza por el Estatuto del Niño, Niña y Adolescente (*Estatuto da Criança e do Adolescente* - Ley 8.069/1990)[103] mediante políticas, justicia especializada y medidas de prevención y respuesta. En materia de datos personales, la LGPD (Ley 13.709/2018)[104] dedica un artículo al tratamiento de datos de la niñez, imponiendo el estándar del interés superior para cualquier actividad de tratamiento de sus datos.

En Perú, el Código de Niños y Adolescentes (Ley 27337)[105] también enmarca la protección integral y define las categorías etarias. La Ley de Delitos Informáticos (Ley 30096)[106] tipifica conductas de riesgo digital como el *grooming* y ha sido reforzada recientemente para promover el uso seguro y responsable de tecnologías por parte de NNA. A su vez, la Ley de Protección de Datos Personales (Ley 29733)[107] reconoce la necesidad de medidas especiales en el tratamiento de datos de personas menores de 18 años, a ser desarrolladas reglamentariamente y con enfoque de derechos.

En Argentina, la Ley de Protección Integral de los Derechos de las Niñas, Niños y Adolescentes (Ley 26.061)[108], de 2005, establece el sistema de protección a estas personas a nivel federal. En la esfera criminal, el Código Penal (Ley 26.904)[109] criminaliza el acoso a personas con menos de 18 años por medios electrónicos y la Ley 27.590 (también conocida como Ley Mica Ortega)[110] crea un programa nacional de prevención y concientización sobre *grooming* o ciberacoso. Por su parte, la Ley 25.326, de protección de datos, no contiene un capítulo específico para NNA, pero la AAIP emitió guías y recomendaciones para su resguardo en entornos digitales[111].

Los hallazgos sugieren que, aun con leyes existentes, persiste una brecha crítica entre el reconocimiento formal y la protección efectiva. La explotación de estéticas que hipersexualizan a niñas revela cómo se entrelazan las violencias de género y las ejercidas contra la infancia, generando daños superpuestos. Superar esta brecha requiere instituciones sólidas, medidas técnicas verificables y obligaciones claras tanto para plataformas como para las autoridades, a fin de que los derechos no queden meramente enunciados sino efectivamente garantizados.

102. Disponible en: **https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm**

103. Disponible en: **https://www.planalto.gov.br/ccivil_03/leis/l8069.htm**

104. Disponible en: **https://www.planalto.gov.br/ccivil_03/leis/l8069.htm**

105. Disponible en: **https://www.mimp.gob.pe/files/direcciones/dgnna/Lectura_3_Nuevo_codigo_de_los_ni%C3%B1os_y_adolescentes.pdf**

106. Disponible en: **https://lpderecho.pe/ley-delitos-informaticos-ley-30096/**

107. Disponible en: **https://www.gob.pe/institucion/congreso-de-la-republica/normas-legales/243470-29733**

108. Disponible en: **https://www.argentina.gob.ar/normativa/nacional/110778/texto**

109. Disponible en: **https://servicios.infoleg.gob.ar/infolegInternet/anexos/15000-19999/16546/texact.htm**

110. Disponible en: **https://www.argentina.gob.ar/normativa/nacional/ley-27590-345231/texto**

111. Para más información, ver: **https://www.argentina.gob.ar/aaip/nuestro-mundo-digital-guia-pedagogica-y-guia-para-adolescentes**

VOLVER AL ÍNDICE

6

RECOMENDACIONES

Esta sección reúne un conjunto de recomendaciones operativas y concretas para enfrentar las vulneraciones a derechos identificadas en los hallazgos de esta investigación. Se organizan por ejes temáticos y, en cada uno, se proponen acciones generales, con medidas específicas por país cuando corresponda.

El enfoque prioriza las medidas de atención, protección y reparación específicas a las víctimas de los ataques y vulneraciones de derechos identificados; la integración sustantiva de las perspectivas de género y de NNA; el fortalecimiento de las instituciones para la aplicación efectiva de las leyes existentes; y la gobernanza y responsabilidad del sector público sobre datos. Dado el carácter transfronterizo del mercado ilegal de datos, se incorporan también medidas de cooperación regional, así como obligaciones reforzadas para plataformas. Todo bajo estándares del derecho internacional, basados en la proporcionalidad, el debido proceso y los derechos humanos.

6.1 Atención y reparación a víctimas con datos en circulación en el mercado ilegal

Los casos identificados por la investigación, así como los no mapeados que circulan en mercados ya establecidos, muestran que, además de ajustar arquitecturas legales e institucionales, es imprescindible situar a las personas afectadas por la compra y venta de sus datos en el centro. Una respuesta eficaz requiere servicios accesibles, gratuitos y sensibles, con rutas claras de investigación y actuación coordinadas entre actores como autoridades, plataformas, operadores de pago y telecomunicaciones. En otras palabras, y en concordancia con el Protocolo La Esperanza[112], la respuesta a víctimas debe ser integral, sensible al trauma y centrada en los derechos de las personas afectadas.

Por eso, se recomienda:

- Realizar operaciones de investigación y mapeo integral del mercado ilegal de datos en Telegram para dimensionar su escala, estructura y daños; conformando equipos conjuntos entre autoridades de protección de datos, fiscalías, equipo de Respuesta a Incidentes de Seguridad Informática CERT (*Computer Emergency Response Team*, en inglés) CSIRT (*Computer Security Incident Response Team*, en inglés) defensorías y con el apoyo de la sociedad civil y la academia.

- Garantizar patrocinio jurídico gratuito cuando sea el caso y representación especializada para solicitar administrativa o judicialmente medidas cautelares, incluyendo: retiro de contenidos, órdenes de no contacto, prohibición de difusión, preservación de evidencia y, cuando corresponda, cambio expedito de documentos y credenciales comprometidos.

- Proveer apoyo desde equipos técnicos de respuesta que dimensionen la extensión del daño, identifiquen los sistemas y entornos afectados, configurando alertas de nuevas apariciones y restableciendo accesos privados y seguros.

112. Para más información, ver: **https://esperanzaprotocol.net/wp-content/uploads/2025/05/PLE-Digital-Espanol.pdf**

- Desplegar equipos psicosociales con enfoque de género y niñez para atención integral y sensible al trauma, con protocolos claros de confidencialidad, consentimiento informado y derivación segura. Asegurar accesibilidad para personas con discapacidad y cobertura en idiomas indígenas cuando sea pertinente.

- Operacionalizar el derecho a la supresión y desindexación donde corresponda, garantizando la remoción de contenidos en plazos perentorios.

- Notificar de manera proactiva a personas potencialmente afectadas cuando se verifique una filtración con datos personales, informándoles los riesgos, las medidas adoptadas y los pasos de protección recomendados, y ofrecer asistencia inmediata. Priorizar a NNA, mujeres y población LGBTQIA+, así como a personas en situación de vulnerabilidad por otras razones, como las étnico-raciales o territoriales.

- Estandarizar protocolos de preservación de evidencia y cadena de custodia para evitar que las víctimas tengan que volver a exponer información sensible. Proveer canales seguros de envío de pruebas, minimizar la recolección de datos adicionales y limitar la retención al tiempo estrictamente necesario.

- Instalar mecanismos de quejas y apelaciones accesibles para cuando la respuesta estatal o de plataformas sea tardía o insuficiente, con revisión independiente, plazos definidos y obligación de motivar cada decisión.

6.2 Violencia de género facilitada por tecnologías

La venta y uso de datos personales potencia patrones de control, extorsión y silenciamiento que ya afectan de manera desproporcionada a mujeres y personas LGBTQIA+. Para su protección, se requiere una integración efectiva de la perspectiva de género a políticas de protección de datos y ciberseguridad, así como medidas integrales, órdenes de protección digitales y servicios de apoyo.

- Reconocer a la VGFT como violación de derechos humanos y violencia de género, garantizando que las leyes estén integradas con medidas de protección digital a víctimas de ataques, como la remoción rápida de contenido dañino, bloqueo de contacto, prohibición de difusión, y preservación de evidencia. Esto es sobre todo clave en el caso de Brasil, que no reconoce explícitamente en su ordenamiento legal la violencia de género facilitada por las tecnologías como modalidad de violencia de género.

- Establecer protocolos intersectoriales entre órganos públicos como las autoridades de protección de datos y los CERT/CSIRT nacionales, policías, fiscalías, funcionarias y funcionarios de la justicia y de los órganos de atención a víctimas de violencia de género para casos con uso de datos comprados y/o filtrados, de manera que haya una ruta única de atención integrada y protectora, según los estándares del Protocolo la Esperanza[113].

113. Ibid

- Brindar formación obligatoria y continua en temas de género y violencia digital para autoridades de protección de datos y ciberseguridad, ministerios públicos, judicatura y defensorías.

- Establecer el monitoreo y publicar datos desagregados por género e identidad en registros de incidentes, con informes públicos.

6.3 Protección a las infancias

NNA son personas en etapa de desarrollo físico, psíquico, emocional y social, que tienen derecho a protección integral y especifica. La venta de sus datos y el uso de estéticas hipersexualizadas en los grupos y canales de Telegram refuerzan prácticas ilícitas y aumentan los riesgos para su integridad y la de sus familias. Se requieren reglas de diseño, restricciones comerciales y servicios de protección adecuados a la edad.

Por eso, se recomienda:

- Establecer normativas aplicables a servicios y productos digitales dirigidos o accesibles a NNA que garanticen la privacidad y seguridad máxima por defecto, minimización estricta de datos tratados y medidas reforzadas de ciberseguridad.

- Exigir evaluaciones de impacto específicas a los derechos de la niñez obligatorias para sistemas públicos y también privados que traten datos de NNA y para servicios digitales masivos usados por NNA. Incluir en la metodología de estas evaluaciones de impacto etapas de consulta significativa con NNA y especialistas.

- Garantizar que los servicios de tecnología orientados a la educación y aplicados a bases de datos de escuelas y de secretarías de educación prioricen la seguridad y privacidad por diseño, prohibiendo la recolección de datos innecesarios y el rastreo de terceros; limitando accesos, auditando proveedores y contratos, definiendo calendarios de retención y borrado de datos, y ofreciendo alternativas no digitales para evitar exclusión. Asimismo, capacitar a docentes y equipos escolares en protección, respuesta a incidentes y apoyo psicosocial.

- Implementar líneas de ayuda especializadas y equipos psicosociales con protocolos de mitigación de daños digitales a NNA o brindar capacitación en la materia a equipos existentes en temas digitales.

6.4 Cumplimiento legal y autonomía institucional

Brasil, Perú y Argentina cuentan con leyes de protección de datos, aunque con distintos grados de desarrollo y en algunos casos sin disposiciones específicas para el sector público. También cuentan con estrategias de ciberseguridad y normas penales relativas a delitos informáticos. Sin embargo, la evidencia muestra que la existencia de estas leyes no basta para garantizar una protección amplia de la ciudadanía frente a los mercados de compra y venta de datos en Telegram. La discusión, por tanto, debe ir más allá de lo normativo y centrarse en la aplicación efectiva de las leyes, así como en la necesidad de dotar a las autoridades

de atribuciones y capacidades suficientes para supervisar y sancionar, incluido al propio Estado cuando incurra en vulneraciones derechos.

Por tanto, se recomienda:

- Garantizar la autonomía institucional de autoridades de protección de datos y de ciberseguridad frente a los gobiernos. Dicha autonomía debe incluir mecanismos de supervisión civil independiente, rendición de cuentas y protección frente a interferencias políticas. Eso es especialmente relevante en los casos de Perú y Argentina, donde las autoridades se encuentran integradas bajo la arquitectura institucional de ministerios del propio Estado y de inteligencia, respectivamente.

- Garantizar el debido presupuesto plurianual de las autoridades de protección de datos y de los CERT/CSIRT nacionales, con reglas claras que limiten la injerencia política externa. Asegurar a estas instituciones escalas salariales competitivas y una carrera técnica que permita atraer y retener perfiles claves, de modo que tengan efectiva capacidad de supervisar y responder a incidentes. Eso es clave en el caso de Brasil, cuya autoridad de protección de datos es independiente, pero tiene limitada capacidad de actuación debido a limitaciones presupuestarias y de personal.

- Otorgar institucionalmente facultades sancionadoras efectivas frente a entes privados y también públicos. Ordenar la publicación de sanciones y de medidas adoptadas a fin de generar efectos disuasorios y fortalecer la transparencia.

- Capacitar juzgados y fiscalías en temas como cibercrimen, protección de datos y violencia digital, con protocolos de cadena de custodia y guías para evidencia electrónica.

- Establecer canales seguros para personas denunciantes (*whistleblowers*, en inglés), que garanticen confidencialidad, protección frente a represalias y mecanismos de seguimiento público sobre las medidas implementadas.

- Publicar informes periódicos y tableros públicos sobre incidentes de seguridad y filtraciones que afecten datos de la ciudadanía, en formatos abiertos y accesibles, con protección de identidad mediante medidas de anonimización y pseudonimización. Desagregar la información por indicadores como género y franjas etarias para orientar políticas públicas y focalizar medidas de prevención y reparación.

6.5 Gobernanza de datos públicos y responsabilidad de los Estados

La evidencia sugiere que es posible que una parte relevante de los datos comercializados provenga de bases de datos estatales o de servicios públicos conectados a ellas. La digitalización acelerada de los Estados sin controles equivalentes de seguridad, auditoría y transparencia ha creado superficies de ataque y de abuso interno que requieren reglas y capacidades reforzadas, distintas a las del sector privado.

Por eso, se recomienda:

- Establecer un régimen legal reforzado para el sector público: revisión o reforma de leyes o reglamentos específicos que establezcan responsabilidades diferenciadas a los Estados para el tratamiento de datos personales. Además de transparencia reforzada, esas normativas deben establecer medidas de restricción al uso secundario de datos, reforzar principios como lo de minimización, garantizar el ejercicio de derechos y prohibir consultas masivas sin justificación caso a caso.

- Minimización de los datos recolectados y almacenados por instituciones públicas, limitándolos a los principios de la necesidad y adecuación.

- Políticas de ciberseguridad en las instituciones públicas que gestionan bases de datos, incluyendo adecuada gestión de accesos, aplicando el principio de mínimo privilegio de modo que cada persona funcionaria solo acceda a la información estrictamente necesaria para cumplir sus funciones; así como la revocación inmediata de credenciales cuando cambian de puesto o dejan la institución. Además, implementar mecanismos de monitoreo mediante alertas en tiempo real para detectar consultas masivas y automatizadas inusuales en las bases de datos.

- Los registros de datos personales deben estar cifrados tanto en tránsito como en reposo, reduciendo así la probabilidad de exposición. También se debe separar los entornos de prueba de los entornos de producción y aplicar técnicas de enmascaramiento o anonimización de datos en aquellas consultas que no requieran mostrar información completa.

- Realización de ejercicios de penetración regulares en sus sistemas para identificar brechas antes de que sean explotadas por terceros, estas pruebas deben contemplar tanto escenarios de ataque externo como simulaciones de amenazas internas, garantizando que no se recolecten ni se procesen más datos personales de los estrictamente necesarios para su ejecución y análisis, conforme al principio de minimización.

- Notificación obligatoria de brechas al tratarse de datos públicos, con plazos breves, registros públicos de incidentes, análisis de causa raíz y plan de remediación verificable.

- Auditorías externas periódicas sobre bases de datos públicas, sobre todo las de registros críticos como de identidad, licencias, educación, salud, crédito y programas sociales, y publicación de sus resultados. Estas auditorías deben incluir, además de una evaluación técnica de seguridad, evaluaciones de impacto en derechos humanos y transparencia activa sobre sus hallazgos, conforme a los lineamientos del Protocolo La Esperanza[114].

- Contratación y compras seguras: agregar a los contratos públicos relacionados a los sistemas de guarda de datos cláusulas de ciberseguridad y privacidad por diseño, y priorizar contrataciones de software de código abierto, incluyendo auditorías públicas del código, transparencia de dependencias e interoperabilidad basada en estándares abiertos.

114. Ibid

6.6 Gobernanza de plataformas digitales

Los hallazgos indican que en Telegram, sin perjuicio de que prácticas similares se verifiquen en otras plataformas, la compra y venta de datos personales se articula mediante *bots*, pasarelas de pago y opacidad operativa. En este marco resulta clave pensar la responsabilidad de las plataformas desde estándares de derechos humanos.

Esto implica avanzar hacia una gobernanza basada en principios de legalidad, necesidad y proporcionalidad, con garantías del debido proceso y mecanismos de transparencia significativa mediante informes y auditorías accesibles. Asimismo, requiere una debida diligencia reforzada para *bots* y sistemas automatizados, la verificación de desarrolladores y de los flujos de monetización, la incorporación de límites y salvaguardas técnicas proporcionales al riesgo y; la existencia de mecanismos efectivos de reparación para las víctimas, preservando a la vez la privacidad y la libertad de expresión.

Por eso, se recomienda:

- Habilitar sistemas accesibles para que las personas usuarias puedan reportar *bots* sospechosos, además de implementar mecanismos de detección para identificar *bots* que accedan o procesen datos personales, con el acompañamiento de organizaciones defensoras de derechos humanos.

- Publicar reportes periódicos de remoción y cumplimiento de órdenes legales y judiciales con datos agregados y desagregados por tipo de abuso, género y franja etaria cuando corresponda.

- Habilitar un canal de respuesta rápida para órdenes judiciales de remoción de contenido, acreditando organizaciones de la sociedad civil y academia como *trusted flaggers*, comprometiendo plazos perentorios para la mitigación de riesgos altos y documentando los criterios de priorización y los resultados de cada intervención.

- Fortalecer la coordinación entre agencias policiales, pasarelas de pago y servicios financieros para identificar flujos vinculados a la comercialización ilícita de datos personales, basándose en análisis de riesgo y en investigaciones o denuncias formales, evitando el rastreo indiscriminado de transacciones.

- Exigir transparencia operativa para *bots* y automatizaciones, publicando términos específicos de uso, reglas de recopilación y tratamiento de datos, fuentes de entrenamiento cuando se use IA y exponiendo métricas de seguridad y cumplimiento, con auditorías independientes y términos accesibles al público.

- Garantizar mecanismos efectivos de reparación para víctimas de vulneraciones en sus entornos, ofreciendo rutas claras de denuncia dentro de la plataforma, priorizando la remoción de contenido que revele datos sensibles y permitiendo la desindexación y la prevención de su re-publicación, con salvaguardas para la libertad de expresión y el debido proceso.

- Aplicar el principio de proporcionalidad en todas las medidas, minimizando los impactos sobre personas usuarias que hacen un uso lícito de los servicios, preservando la privacidad mediante el uso de cifrado extremo a extremo y

combinando herramientas técnicas y de gobernanza que sean necesarias y adecuadas para el fin perseguido, evaluando regularmente su eficacia y posibles efectos adversos.

• Designar un responsable legal con domicilio y facultades suficientes en cada país donde operen las plataformas, inscribirlo ante las autoridades y reguladores correspondientes y mantener un punto de contacto para autoridades y personas usuarias. Garantizar que dicho responsable pueda recibir notificaciones y órdenes judiciales o administrativas y cumplir los plazos y requisitos locales, a la vez que asegura la adhesión a estándares internacionales y regionales de derechos humanos.

6.7 Cooperación regional y transfronteriza

El mercado ilegal de datos y las dinámicas de violencia identificadas en esta investigación operan en muchos casos a escala transfronteriza. La cooperación regional, en este sentido, es clave. Para eso, se recomienda:

• Conformar equipos conjuntos de investigación regional para venta de datos, *doxxing* y extorsión, estableciendo criterios de activación, objetivos, plazos y métricas de éxito.

• Publicar informes regionales de transparencia con estadísticas comparables sobre incidentes, tiempos de respuesta, sanciones y reparación a víctimas, evaluando impactos, salvaguardas de libertad de expresión y privacidad y documentando metodologías.

• Fortalecer redes y organismos de colaboración regional en temas de protección de datos y ciberseguridad, como la Red Iberoamericana de Protección de Datos y la Organización de los Estados Americanos, como plataformas operativas para producción de evidencias y coordinación de políticas en casos de vulneración de derechos como el de compra y venta de datos personales, así como de filtraciones de bases de datos públicas, creando grupos de trabajo permanentes con metas y cronogramas, asignando presupuesto para soporte técnico forense.

• Establecer protocolos de preservación de evidencia digital y circulación transfronteriza de esas evidencias basados en estándares de derechos humanos y en parámetros de legalidad, necesidad y proporcionalidad.

• Definir salvaguardas para investigaciones en contextos transfronterizos.

• Garantizar protección y reparación transfronteriza para víctimas cuando sea el caso, homologando órdenes de protección digitales entre países y activando redes institucionales de apoyo a víctimas cuando la persona afectada esté fuera de su país.

• Garantizar que toda cooperación impulsada incorpore evaluaciones de impacto en derechos humanos y mecanismos de apelación y rendición de cuentas, publicando resúmenes de operaciones, resultados y lecciones aprendidas sin exponer a víctimas ni comprometer investigaciones en curso.

WWW.DERECHOSDIGITALES.ORG