IDENTIDADES **À VENDA**

O mercado ilegal de compra e venda de dados pessoais latino-americanos no Telegram

Derechos Digitales
AMÉRICA LATINA

Derechos Digitales
AMÉRICA LATINA

Tradução para português:
Dafne Melo
Desenho e diagramação:
El Maizal

Esta é uma publicação da Derechos Digitales, uma organização independente sem fins lucrativos, fundada em 2005, que tem como missão a defesa, promoção e desenvolvimento dos direitos humanos em ambientes digitais na América Latina. O trabalho de pesquisa que deu origem a essa publicação ocorreu entre outubro de 2024 e novembro de 2025.

SUMÁRIO

RESUMO EXECUTIVO

Este relatório documenta a existência e funcionamento de um mercado ilegal de compra e venda de dados pessoais na América Latina através da plataforma Telegram. A partir de uma pesquisa empírica realizada entre outubro de 2024 e fevereiro de 2025 no Brasil, Peru e Argentina, foram identificados vinte e sete grupos e canais ativos dedicados à comercialização de informação pessoal. Os resultados revelam um ecossistema altamente automatizado, operado por *bots* e esquemas de pagamento digital, que permite o acesso imediato a dados pessoais -inclusive dados sensíveis- como documentos de identidade, endereços, informações financeiras, de emprego, de saúde ou históricos familiares, transformando a identidade das pessoas em um insumo de valor econômico.

Os indícios observados sugerem que algumas das informações em circulação podem ter origem, direta ou indireta, em bases de dados públicas ou registros oficiais. Embora não seja possível afirmar isso com certeza, a similaridade em formatos, terminologia e estruturas técnicas, juntamente com a presença de marcas institucionais, aponta para potenciais vulnerabilidades na gestão da informação estatal. Esse fenômeno se desenvolve em um contexto regional de digitalização acelerada de serviços públicos sem mecanismos equivalentes de segurança, auditoria ou transparência, o que amplia a superfície de exposição e os riscos de uso secundário -e até mesmo imprevisto- dos dados.

Os resultados da pesquisa revelam três dimensões que apontam para uma fragilidade estrutural característica da América Latina, e que requerem mais pesquisas para estabelecer suas origens, causas e soluções. A primeira é normativa: embora os três países possuam leis de proteção de dados, estratégias de cibersegurança e marcos penais para crimes cibernéticos, persistem lacunas significativas, especialmente no que diz respeito ao processamento de dados pelo setor público. A segunda é institucional: as autoridades responsáveis pela aplicação dessas normas geralmente carecem de independência, recursos e capacidade para fiscalizar o próprio Estado. A terceira relaciona-se à segurança da informação: os órgãos públicos responsáveis pela gestão de grandes volumes de informação carecem de políticas de segurança robustas, o que, aliado a um histórico extenso e amplamente conhecido de vazamentos de dados, reflete a ausência de uma cultura de proteção da informação sólida na região e a consequente necessidade de seu aprofundamento.

Os riscos derivados deste mercado ilegal não são meramente técnicos. A disponibilidade e circulação de dados pessoais no Telegram potencializou formas de violência, incluindo a violência de gênero facilitada por tecnologias (VGFT) e a exposição de crianças e adolescentes a novas formas de violação a seus direitos. Nos três países, foram identificados casos concretos em que dados pessoais obtidos ou divulgados

no Telegram foram usados para extorquir, assediar ou ameaçar mulheres, além de evidências da venda e uso de informações que afetam diretamente crianças, adolescentes e suas famílias. Esses eventos demonstram como a exploração de dados se cruza com estruturas preexistentes de desigualdade e poder, tornando-se um mecanismo de controle, silenciamento e revitimização.

Em conjunto, as conclusões demonstram que a região enfrenta um déficit estrutural na tradução dos quadros regulamentares existentes em garantias de proteção efetivas. Superar essa lacuna exige fortalecer a governança e a segurança dos dados públicos, dotar as autoridades competentes de autonomia e recursos, e integrar abordagens centradas em gênero e na infância nas políticas de segurança cibernética e proteção de dados. A dimensão transnacional do fenômeno também exige cooperação regional, mecanismos de responsabilização e ações decisivas por parte das plataformas tecnológicas. Em resposta, este relatório oferece um conjunto de recomendações concretas cuja orientação é fortalecer as capacidades institucionais, garantir reparações às vítimas e promover processos de digitalização a nível estatal ancorados nos direitos humanos.

VOLTAR AO SUMÁRIO

1 INTRODUÇÃO

A venda de dados pessoais tornou-se um negócio lucrativo na economia digital clandestina. Documentos de identidade, endereços, números de telefone, informações bancárias e até mesmo registros médicos circulam sem consentimento, expondo milhões de pessoas a diversos tipos de riscos.

Inicialmente, esse comércio ilícito se concentrava em fóruns clandestinos da *dark web*, em que agentes maliciosos compravam e vendiam bases de dados filtradas tanto de governos como de empresas privadas. No entanto, nos últimos anos, essa atividade migrou para espaços digitais mais acessíveis, incluindo o Telegram, uma plataforma que oferece aos vendedores maior facilidade de conexão com os compradores sem a necessidade de conhecimento avançado.

A exposição de dados pessoais constitui uma séria ameaça à segurança dos indivíduos e ao exercício de seus direitos fundamentais. Roubo de identidade, violações de contas bancárias, fraudes, extorsão e ameaças digitais estão entre os impactos potenciais enfrentados por indivíduos que veem suas informações comprometidas. Essas experiências podem gerar impactos emocionais, financeiros e de desconfiança em relação aos ambientes digitais e à participação neles.

Na América Latina, a situação se agrava devido a condições estruturais preexistentes. Fatores como fragilidade institucional, deficiências na gestão de dados e lacunas tecnológicas criam um ambiente fértil para a exploração digital. Essa situação é agravada pela falta de uma cultura robusta de proteção de dados e segurança cibernética, bem como pelo desenvolvimento relativamente recente e desigual da legislação nessa área, o que limita a capacidade de prevenir e remediar abusos.

Essas condições estão interligadas com desigualdades históricas -socioeconômicas, de gênero, étnicas ou territoriais- que fazem com que os impactos recaiam desproporcionalmente sobre as populações em situação historicamente vulnerável. Assim, o tráfico de dados não constitui apenas uma ameaça técnica, mas também uma forma contemporânea de violência que aprofunda as desigualdades históricas.

Este relatório busca evidenciar a existência e funcionamento do mercado de comercialização ilegal de dados pessoais na América Latina através da infraestrutura do Telegram. Com base em pesquisa empírica apoiada por observação não participante de grupos e canais dentro da plataforma, foram identificados padrões, modos de operação, preços e tipos de dados, permitindo traçar um mapa dessa economia digital ilegal.

Além de documentar esse fenômeno, o principal objetivo é gerar uma consciência crítica sobre seu impacto e exigir respostas urgentes, bem como mecanismos de reparação. A falta de regulamentação eficaz, a fragilidade das políticas públicas em matéria de proteção de dados e cibersegurança, e a inação das plataformas digitais têm o potencial de contribuir para a expansão dessas práticas. Diante desse cenário, são necessárias respostas abrangentes sob a perspectiva dos direitos humanos: centradas nas pessoas, com mecanismos de responsabilização e reparação, e atenção especial aos setores vulneráveis.

Este relatório se divide em quatro seções. A primeira seção aborda a infraestrutura do Telegram e explica as razões pelas quais se converteu em um espaço propício para a compra e venda ilegal de dados. O segundo detalha a metodologia utilizada na pesquisa empírica. A terceira seção apresenta as conclusões, com foco em grupos e canais de três países da região: Brasil, Peru e Argentina. Além de identificar a dinâmica de vendas observada, são incluídos aspectos relevantes do contexto sociotécnico, político e jurídico de cada país. Por fim, são apresentadas recomendações, dirigidas principalmente às autoridades nacionais desses países, embora relevantes para toda a região, em relação aos casos identificados e à necessidade de estruturas e infraestruturas regulatórias robustas e autônomas para a implementação. Assim, também são formuladas propostas para órgãos regionais, considerando o caráter transfronteiriço das políticas de proteção de dados e segurança cibernética, bem como a alta probabilidade de que essas práticas se espalhem para outros países da América Latina.

VOLTAR AO SUMÁRIO

2

TELEGRAM COMO MERCADO ILÍCITO

O Telegram é um dos aplicativos de mensagens instantâneas mais utilizados no mundo, com mais de um bilhão de usuários[1]. Seu crescimento também se acelerou na América Latina, onde países como Brasil, México e Colômbia[2] lideram o número de downloads na região. Lançado em 2013 pelos irmãos russos Pavel e Nikolai Durov[3], inicialmente Telegram foi concebido como uma alternativa segura e privada frente a outras plataformas, ao se apresentar como um espaço de comunicações sem vigilância estatal.

Diferente de outros aplicativos, o Telegram permite criar grupos com até 200.000 membros e enviar arquivos de até 2 GB. Sua estrutura foi projetada para facilitar a criação de espaços de interação massivos, com poucos controles de moderação ou restrições de conteúdo.[4], o que cria um ambiente favorável para a disseminação de informações em larga escala. Essas funcionalidades não apenas incentivam a formação de comunidades e a troca massiva de links, mas também tornaram o Telegram uma plataforma atraente para múltiplos usos, inclusive ilegais.

Diferentemente de outros aplicativos de mensagens, o Telegram não criptografa as mensagens de ponta a ponta por padrão; apenas os "chats secretos" possuem essa proteção, que precisa ser ativada manualmente e não está disponível para grupos ou canais. Além disso, a plataforma armazena conversas, metadados e dados do usuário (como nome, número de telefone, contatos e endereço IP) em seus serviços em nuvem. Essas limitações contradizem parcialmente a promessa de privacidade. No entanto, o Telegram mantém atraente para aqueles que buscam um certo grau de anonimato em interações superficiais, já que não exige a exibição de um número de telefone e permite que os usuários operem exclusivamente com um nome de usuário.

Além da comunicação direta entre usuários, o Telegram facilita a interação em massa por meio de grupos e canais, cada um com recursos projetados para diferentes tipos de comunicação. Os grupos são projetados para interação em tempo real entre várias pessoas, chamadas de "membros", que podem participar ativamente enviando mensagens, compartilhando arquivos e vendo quem mais integra o grupo. Esses podem ser públicos, visíveis no buscador de Telegram, ou privados, acessíveis

1. Para mais informação, ver: **https://telegram.org/faq/es**

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

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

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

somente mediante um link de convite. Os canais, por outro lado, são projetados para comunicação unidirecional: apenas os administradores podem postar mensagens, enquanto aqueles que entram atuam como "assinantes". Diferentemente dos grupos, os inscritos não podem ver quem mais está no canal, apenas o número total de inscritos.

Um dos elementos centrais do ecossistema Telegram -tanto em usos legítimos quanto ilícitos- é o uso de *bots*: programas automatizados capazes de executar tarefas sem intervenção ou supervisão humana direta. Funcionam mediante comandos predefinidos, se integrando com bases de dados externas para entregar resultados instantaneamente. Embora originalmente concebidos para melhorar a experiência das pessoas usuárias (por exemplo, moderando chats, enviando lembretes ou facilitando interações em canais de informação), na prática muitos deles foram adaptados para fins ilícitos[5].

No caso da compra e venda de dados pessoais, os *bots* permitem acesso rápido a informações, incluindo dados sensíveis. Basta digitar um número de identificação, nome completo ou número de telefone no chat do *bot* para receber automaticamente seu endereço, informações familiares, detalhes de emprego e histórico criminal ou financeiro. Essa automatização facilita o acesso e a circulação de informações pessoais fora dos marcos de proteção legal, o que incrementa os riscos de uso indevido, roubo de identidade ou violação de direitos em contextos marcados por grandes lacunas de segurança institucional[6].

Considerando o tema deste relatório, é importante mencionar que, nos últimos anos, o Telegram tem sido associado a eventos de grande repercussão relacionados a atividades ilícitas. Em agosto de 2024, Pavel Durov foi detido[7] em Paris no marco de uma pesquisa sobre delitos facilitados pela plataforma, como a distribuição de material de abuso sexual infantil e tráfico de drogas. Poucos meses depois, em novembro do mesmo ano, uma pesquisa[8] revelou o funcionamento de um grupo com mais de 70.000 homens no Telegram que compartilhavam estratégias para drogar e agredir mulheres sexualmente.

Esse episódio marcou uma virada na política histórica do Telegram de não cooperar com agentes estatais. Após a detenção de Durov, a plataforma anunciou[9] que começaria a colaborar com autoridades sob ordem judicial, entregando dados como o número de telefone ou o endereço de IP de pessoas usuárias.

5. Flare (2023). The Typology of Illicit Telegram Channels. Disponível em: **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. Disponível em: **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. Disponível em: **https://www.publico.es/mujer/violencia-machista/investigacion-destapa-red-70-000-hombres-telegram-comparten-estrategias-drogar-agredir-sexualmente-mujeres.html**

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

Casos como este reforçam as preocupações sobre a postura passiva da plataforma diante de formas organizadas de violência[10]. A existência de ferramentas de privacidade é fundamental para garantir a liberdade de expressão, a segurança e a proteção dos usuários, especialmente em contextos de vigilância ou perseguição política. No entanto, é também essencial exigir que as empresas de tecnologia cumpram o seu dever de agir perante os danos que se originam ou são reproduzidos nos seus ambientes. Além da prevenção, devem assumir a responsabilidade pela detecção precoce, mitigação e reparação dos impactos que suas próprias arquiteturas facilitam ou amplificam.

Assim como outras tecnologias voltadas para a proteção da privacidade, o Telegram tem o potencial de servir tanto para a proteção legítima de direitos quanto para facilitar abusos e perpetuar a violência. Este relatório não pretende desqualificar práticas ou espaços digitais que defendam a privacidade e o anonimato, uma vez que ambos constituem direitos fundamentais e, ao mesmo tempo, condições que possibilitam o exercício de outros direitos humanos no ambiente digital, como a liberdade de expressão e de associação. Em outras palavras, o potencial de uso duplo não invalida a importância de sua existência, mas exige uma análise crítica de como as decisões de design, governança e transparência impactam seu uso cotidiano.

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. Disponível em: **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/**

VOLTAR AO SUMÁRIO

3 METODOLOGIA

A pesquisa foi realizada entre outubro de 2024 e novembro de 2025, com foco no Brasil, Peru e Argentina. O objetivo foi identificar a dinâmica da comercialização de dados pessoais por meio dos canais e grupos públicos do Telegram na América Latina, em contextos em que as desigualdades estruturais, a fragilidade institucional e a limitada eficácia da proteção de dados amplificam os riscos para os cidadãos.

A abordagem metodológica e o trabalho de campo foram organizados em três fases principais: exploração, observação e análise.

1. A fase de exploração permitiu identificar os espaços públicos onde se realiza a compra e venta de dados dentro do Telegram. Para isso, grupos e canais foram localizados utilizando quatro estratégias: a aplicação da técnica de amostragem em bola de neve (*snowball sampling*)[11], ferramentas de busca automatizadas e manuais no Telegram, bem como o monitoramento de denúncias em redes sociais sobre a venda de dados pessoais.

Com relação às ferramentas de busca automatizadas, foi utilizada uma técnica de extração automatizada de conteúdo público por meio do desenvolvimento de scripts ou códigos personalizados em Python.[12]. Palavras-chave como "venda" ou "dados" foram usadas para identificar grupos e canais potencialmente dedicados à compra e venda de dados pessoais. Essas palavras também guiaram a busca manual dos espaços no buscador de Telegram.

O monitoramento de denúncias nas redes sociais, por sua vez, possibilitou identificar links que levavam a grupos públicos do Telegram relacionados à venda de dados, bem como tornar visíveis as narrativas das pessoas usuárias sobre a exposição de seus dados pessoais e as consequências daí resultantes.

2. Una vez identificados os espaços, foi empregada uma técnica de observação não participante[13] das dinâmicas durante os meses de pesquisa, tanto por meio de monitoramento em tempo real (capturando interações entre vendedores e compradores, bem como mensagens promocionais, respostas automatizadas

11. A aplicação dessa técnica consistiu no rastreamento de links compartilhados dentro dos próprios grupos identificados. Ao se seguir essas conexões, foram descobertos outros espaços similares. Em diversos casos, um canal levava a vários outros, permitindo a construção de uma ampla rede de observação. Essa estrategia se mostrou a mais efetiva para localizar a maioria dos grupos e canais analisados.

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**

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

e comportamentos de consulta), quanto por meio da revisão do histórico de mensagens, detalhando tendências, estruturas organizacionais e mudanças nos métodos de marketing.

3. Finalmente, após a saturação das informações, foi realizada a análise dos dados coletados, com base na construção de um registro comparativo com critérios que incluíam: o alcance dos grupos e canais, seus administradores, os tipos de dados comercializados, o modelo de negócios, os preços e os métodos de pagamento.

Durante a fase de análise, foi realizada uma pesquisa documental para aprofundar o conhecimento sobre os contextos tecnopolítico, social e legais do Brasil, Peru e Argentina em relação à proteção de dados pessoais. Este trabalho possibilitou identificar, entre outros elementos, os atuais marcos regulatórios e os históricos de vazamentos de dados em instituições públicas nesses países.

Por se tratar de uma pesquisa sobre práticas ilegais de compra e venda, foram tomadas medidas para proteger a segurança tanto das pessoas cujos dados poderiam ser comprometidos quanto daqueles que realizaram o trabalho de pesquisa. Nesse marco, foram adotados os seguintes princípios:

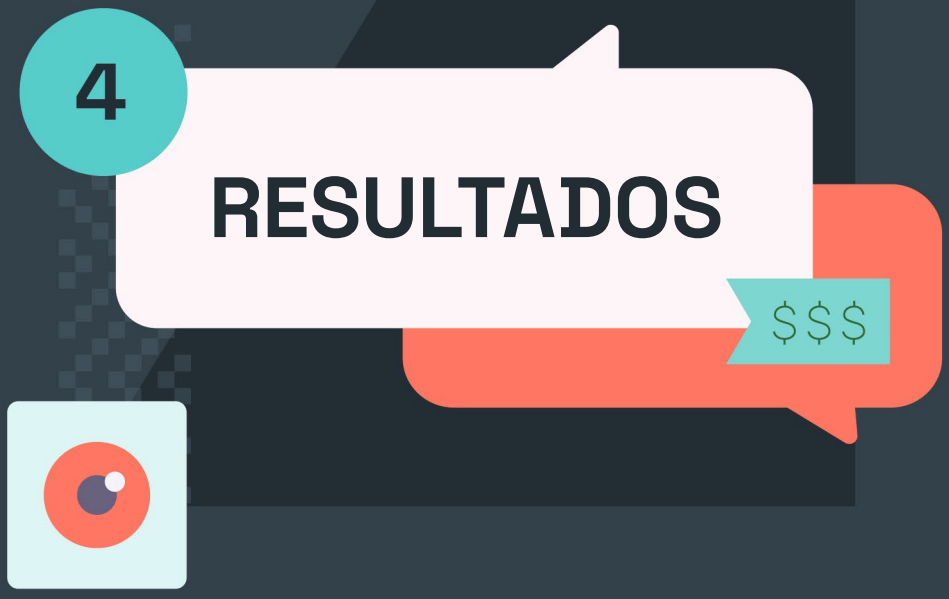
- Este relatório não inclui nomes ou links para grupos ou canais para evitar a reprodução do dano.

- A pesquisa foi de natureza não participante: nenhum contato foi estabelecido com administradores de espaços ou compradores, evitando qualquer forma de interação direta.

- O download automático de arquivos foi desativado porque foram detectados espaços com conteúdo violento e sexual durante a verificação.

VOLTAR AO SUMÁRIO

4 RESULTADOS



A pesquisa concentrou-se em 27 espaços ativos dedicados à comercialização de dados pessoais no Telegram, distribuídos entre o Brasil, o Peru e a Argentina. Durante o trabalho de campo, constatou-se que em diversos grupos e canais dedicados à venda de dados nesses países, também circulavam informações correspondentes a outros territórios, como Venezuela, Bolívia, República Dominicana, Chile e Uruguai, sugerindo que se trata de um fenômeno regional mais amplo que ultrapassa os três países analisados em detalhe. No entanto, a análise que se segue centra-se nos principais achados no Brasil, Peru e Argentina.

Esses 27 espaços foram classificados de acordo com o país de origem, o tipo de interação (grupo ou canal) e o idioma utilizado para a comunicação:

Tabela 1. Descrição dos espaços observados

País	Grupos	Canais	Idioma
Brasil	10	0	Portugués
Perú	8	2	Espanhol
Argentina	1	6	Espanhol

É importante ressaltar que esse número não representa todos os grupos e canais usados para a venda de dados no Telegram, mas sim uma amostra intencional definida de acordo com critérios de acessibilidade, atividade contínua e observação segura, ética e não intrusiva.[14]. Foi dada prioridade à análise de espaços que permitissem a avaliação comparativa sem comprometer a segurança das pessoas usuárias ou daqueles que conduziram a pesquisa.

4.1 Brasil

No Brasil, foram identificados dez grupos, vários deles com um número considerável de membros, revelando um alto nível de tráfego e permanência:

14. Ibid.

Tabela 2. Número de membros dos 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

Nesses grupos, observou-se um alto grau de automação na administração. Todos os espaços analisados possuem pelo menos um *bot* configurado como administrador, o que garante atenção constante às solicitações de dados, sem a necessidade de intervenção e supervisão humana permanente. Essa estrutura facilita o funcionamento do grupo como uma loja ativa 24 horas por dia, com comandos operacionais preestabelecidos para realizar buscas ou compras.

Juntamente com os *bots*, foi identificada a presença de administradores humanos operando sob uma hierarquia reconhecível. São utilizadas etiquetas como "dono", "admin", "suporte" ou "help" [ajuda], que permitem delimitar funções dentro do espaço. A gestão não parece estar centralizada em uma única pessoa, mas sim articulada por uma equipe. Observou-se que essa equipe opera anonimamente por meio do uso desses pseudônimos genéricos e da fragmentação de responsabilidades. Assim, a coordenação ocorre na medida em que cada função cumpre um papel específico sem a necessidade de revelar identidades, o que dificulta o rastreamento.

O modelo de negócio predominante identificado nos grupos é o *freemium*, em que as pessoas usuárias podem realizar um número limitado de consultas gratuitas usando *bots* no Telegram, que geralmente fornecem resultados básicos (por exemplo, nome e **CPF**[15]). No entanto, para acessar dados mais detalhados, como endereço, datas de nascimento, vínculos profissionais ou informações financeiras, é necessário pagar.

Os grupos oferecem diferentes planos dependendo do tempo de acesso (diário, semanal, mensal, trimestral, etc.) e, em alguns casos, por níveis de funcionalidade relacionados ao tipo de dados consultados. Essa abordagem se assemelha a um modelo *freemium* escalonado, no qual funcionalidades limitadas são acessadas gratuitamente e o pagamento é incentivado para obter consultas mais detalhadas. Os preços mais baixos identificados variam de US$ 1 (por uma semana) a US$ 78,80 (por dois anos). Foram identificados promoções e anúncios de compras urgentes (por exemplo, "somente hoje"), refletindo o uso de estratégias típicas de marketing digital adaptadas a um mercado ilícito.

Em relação ao método de pagamento, todos os grupos analisados utilizam o sistema PIX, um mecanismo de pagamento instantâneo lançado pelo Banco Central do Brasil em 2020.[16] Este sistema permite transferências em tempo real entre indivíduos ou empresas, utilizando identificadores únicos (como número de telefone, e-mail, **CPF** ou códigos QR), sem a necessidade de intermediários bancários tradicionais. Embora o PIX tenha sido projetado para garantir a rastreabilidade e reduzir os custos de

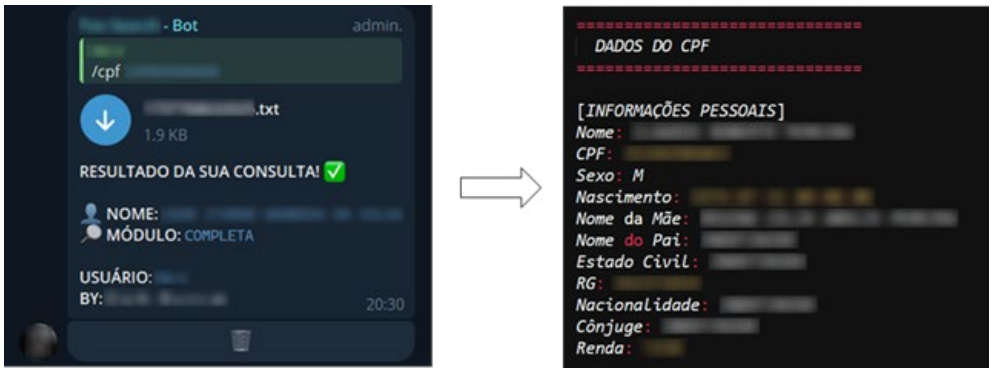
15. **CPF** equivale a "Cadastro de Pessoa Física", o número de identificação fiscal no Brasil.
16. Para mais informação, ver: **https://www.bcb.gov.br/estabilidadefinanceira/pix**

transação, seu uso em contextos informais demonstra como ferramentas financeiras legítimas podem ser exploradas para operações ilícitas ou não regulamentadas. Nos grupos analisados, os pagamentos são geralmente executados usando um código aleatório gerado por meio de plataformas intermediárias, como a **iugu.com**, que integram soluções de faturamento eletrônico.

Observou-se o uso intensivo de *bots* automatizados para a venda de dados pessoais. O comando mais comum é /**cpf**, que permite consultar informações relacionadas ao número de identificação fiscal no Brasil. Ao inserir esse comando seguido do número do **CPF** da pessoa, o *bot* gera um formulário estruturado que pode ser baixado em formato .txt, o qual revela imediatamente os dados pessoais vinculados ao **CPF**.

Os dados fornecidos através do comando /**cpf** criam um perfil extremamente detalhado da pessoa consultada (ver Imagem 1). Em primeiro lugar, inclui-se informação de identificação civil: nome completo, RG (Registro Geral), data de nascimento, sexo[17], munícipio e estado de origem. O registro dos **CPF**s é administrado pela **Receita Federal do Brasil**, entidade encarregada da gestão fiscal e tributária e responsável pela base nacional de contribuintes.

Imagem 1. Evidência visual sobre venda de dados através do comando /**cpf**



A execução do comando também fornece acesso a informações econômicas, como uma estimativa da renda mensal da pessoa consultada. Além disso, inclui-se uma categorização do poder aquisitivo em níveis ("baixo", "médio" ou "alto"), juntamente com uma faixa monetária que indica o intervalo de renda estimado. Essa classificação pode ser obtida a partir de registros fiscais ou de consumo e pode ser usada para inferir o status socioeconômico da pessoa afetada, expondo-a a riscos de discriminação, estigmatização e práticas de exclusão ou de busca por vantagens financeiras.

Juntamente com os dados econômicos, o arquivo revela um sistema de pontuação financeira, ou seja, um sistema que classifica a pessoa de acordo com seu nível de

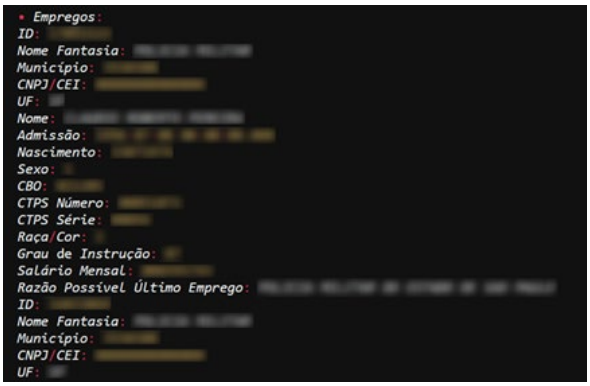
17. Ao longo deste relatório, são feitas referências tanto a "sexo" quanto a "gênero". Essa variação se deve à forma como as informações aparecem em cada grupo ou canal analisado no Telegram e à maneira como os programadores de cada *bot* definem as variáveis em seus sistemas de consulta. Portanto, ambos os termos são mantidos de acordo com seu uso original nas fontes observadas.

risco de crédito. Esse sistema utiliza modelos como CSB[18] e CSBA[19], em que se designam pontuações qualitativas. A presença dessas métricas específicas sugere que os *bots* supostamente estão acessando bancos de dados de crédito institucionais, como o Serasa[20] ou SPC Brasil[21], permitindo construir perfis financeiros detalhados sem o consentimento da pessoa titular.

O perfil financeiro da pessoa consultada parece ser complementado por informações supostamente extraídas do sistema Serasa Mosaic, ferramenta utilizada no Brasil para segmentar consumidores de acordo com seu comportamento e capacidade de consumo.[22] Os registros analisados incluem a descrição do perfil, a classe socioeconômica, diferentes códigos de categorização ("novo", "secundário", "primário") e observações adicionais que podem ser vinculadas ao histórico de compras, pagamentos ou dívidas -campos semelhantes aos disponíveis no próprio sistema Serasa Mosaic-.

Constatou-se que, por meio desse mecanismo de consulta, também é possível acessar informações financeiras relacionadas ao ambiente de trabalho das pessoas. O comando revela a profissão declarada, juntamente com o Código Brasileiro de Ocupações (CBO), uma classificação oficial utilizada no Brasil para padronizar as atividades laborais. Além disso, os *bots* acessam informações de emprego altamente detalhadas, como as encontradas em registros oficiais, como a Carteira de Trabalho e Previdência Social (CTPS), para citar um exemplo. Assim, a estrutura de dados coincide com os campos presentes nesses registros: múltiplas entradas de trabalho por pessoa, nome da empresa empregadora, identificação fiscal (CNPJ), município e estado, datas de admissão, cargo, salário mensal, nível de escolaridade e até variáveis censitárias como raça e sexo (ver Imagem 2). Esses elementos permitem identificar com precisão o nicho profissional da pessoa.

Imagem 2. Evidências visuais da venda de dados contendo informações sobre trabalho.



18. CSB (Credit Score Básico): Indicador utilizado no Brasil que qualifica o risco de credito de una persona em função de variáveis básicas, como histórico de pagamentos e dívidas registradas.

19. CSBA (Credit Score Básico Ampliado): Uma variante do CSB que incorpora mais variáveis, incluindo informações sobre o comportamento do consumidor e seus relacionamentos com instituições financeiras, proporcionando uma análise de crédito mais abrangente.

20. SERASA: Empresa brasileira especializada em análise e gestão de dados financeiros, reconhecida por operar um dos principais bancos de dados de crédito do país, utilizado por entidades para avaliar a capacidade de crédito do consumidor.

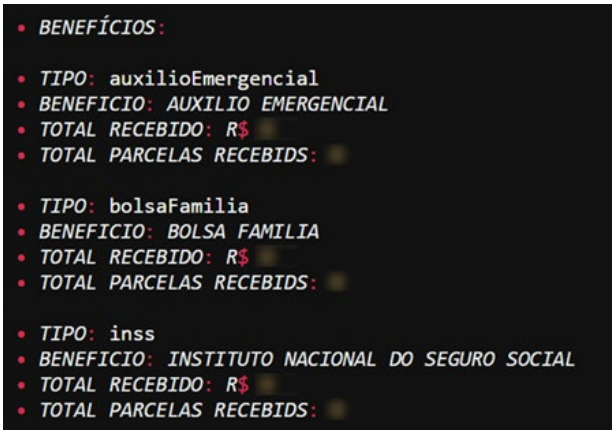
21. SPC Brasil (Serviço de Proteção ao Crédito): Sistema de crédito gerenciado pelas câmaras de comércio brasileiras, que centraliza dados sobre dívidas, pagamentos e comportamento de crédito de pessoas físicas e jurídicas.

22. Disponível em: **https://www.serasaexperian.com.br/solucoes/mosaic/**

Em vários desses registros de emprego, a data de saída aparece como "nula", o que pode indicar que a pessoa ainda trabalha nessa empresa ou que o sistema de origem não atualizou esse campo. No entanto, o ponto mais relevante é que o uso do termo "*null*" é característico de bancos de dados estruturados, como aqueles baseados em SQL[23], o que sugere que a informação provém de sistemas ou respaldos de bases de dados e não de simples capturas ou recolecções informais.

A divulgação do número do Programa de Integração Social (PIS), um identificador fundamental para o acesso a benefícios estatais como pensões, subsídios e fundos de aposentadoria, foi considerada um dado altamente sensível. Além disso, há informações detalhadas sobre o acesso a benefícios sociais como o Auxílio Emergencial (benefício concedido durante a pandemia), o Bolsa Família (programa histórico de transferência de renda) e as contribuições ao Instituto Nacional do Seguro Social (INSS). Em cada caso, são especificados o montante total recebido pela pessoa e o número de prestações efetuadas, o que permite rastrear os padrões de utilização da assistência social (ver imagem 3). Essa informação não apenas expõe o nível de vulnerabilidade econômica da pessoa, mas também permite inferir sobre sua situação de emprego, histórico de renda e grau de dependência de programas estatais, potencialmente expondo-a a fraudes e discriminação direcionadas.

Imagem 3. Evidências visuais sobre venda de dados contendo informação de acesso a benefícios sociais



A estrutura dessas fichas de dados fornecidas pelos *bots* dos grupos analisados possui campos como "tipo: auxilioEmergencial" e "benefício: AUXÍLIO EMERGENCIAL". Isso evidencia uma nomenclatura específica de banco de dados, caracterizada pelo uso de etiquetas no formato "campo:valor" e por convenções técnicas como *camelCase*[24] ("auxilioEmergencial"). Mais uma vez, essas características sugerem que as informações podem ter sido extraídas diretamente de bancos de dados estruturados, possivelmente vazadas ou conectadas em tempo real, do sistema financeiro ou de proteção social.

O mesmo arquivo de consulta por meio do **CPF** também revela linhas telefônicas

23. SQL (Structured Query Language) é uma linguagem padrão usada para gerenciar bancos de dados estruturados, permitindo consultar e atualizar informações armazenadas.

24. Uma convenção de escrita em informática em que a primeira palavra é escrita em minúsculas e as palavras seguintes começam com letra maiúscula, sem espaços ou hífenes.

celulares associadas à pessoa consultada. Para cada linha, são indicados o tipo de serviço e a respectiva operadora de telecomunicações. O aparecimento de múltiplos registros associados à mesma pessoa pode ser devido a uma comparação entre bancos de dados, possivelmente de provedores de serviços móveis ou registros históricos de linhas ativas e inativas.

O acesso aos endereços registrados constitui outra dimensão crítica da exposição de dados. No mesmo arquivo .txt de resposta, são identificados vários registros por pessoa, indicando que os bancos de dados armazenam um histórico de endereços ao longo do tempo. Cada entrada contém informações detalhadas como código postal (CEP), estado federal (UF), município, rua (logradouro), bairro (bairro), número da residência e complemento, permitindo localizar uma pessoa com alta precisão geográfica. Além do endereço atual, o município de nascimento é incluído, o que amplia a rastreabilidade da trajetória de vida da pessoa.

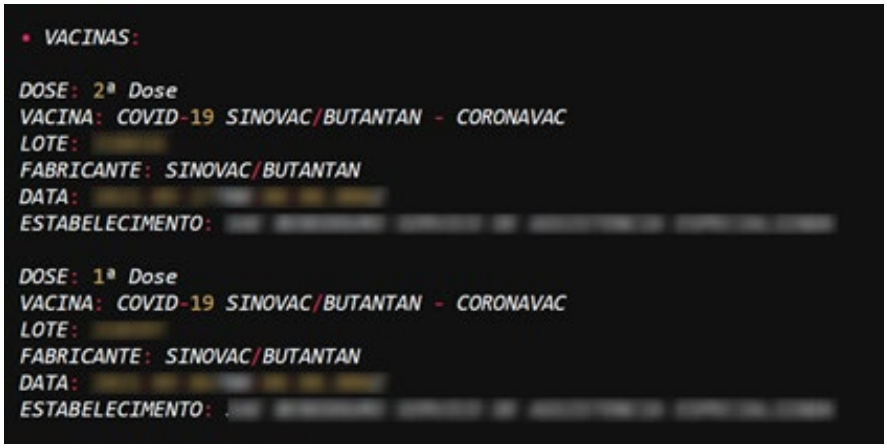
A exposição de vários domicílios permite o rastreamento de movimentos passados e presentes, o que pode levar a riscos de assédio, extorsão ou vigilância. Em contextos como o do Brasil -e, de modo geral, em diversos países da América Latina- onde convergem altos níveis de violência urbana, crime organizado, desigualdade e polarização política[25], esse tipo de vazamento pode expor as pessoas a diversas ameaças: desde fraudes direcionadas e ataques físicos ou digitais até assédio direcionado, motivado por razões políticas, de gênero ou étnicas, entre outras.

A exposição não se limita à pessoa consultada. Os registros analisados também mostram informações sobre sua rede familiar direta (como irmãs, irmãos, sobrinhas, sobrinhos) e outros laços de parentesco. Cada familiar aparece identificado por seu nome completo e número de **CPF**. Além disso, sob o rótulo "vizinhos", os *bots* divulgam dados de pessoas que residem nas proximidades do proprietário consultado. A inclusão desses terceiros amplia o escopo do vazamento e pode facilitar a criação de perfis relacionais, capazes de mapear laços familiares e comunitários, e eventualmente serem combinados com outros dados para fins como fraude direcionada, roubo de identidade, extorsão ou vigilância por atores não estatais.

Outra descoberta alarmante nesse arquivo de texto é a exposição do histórico de vacinação, no qual são apresentados dados estruturados que replicam a lógica de um registro oficial do sistema de saúde brasileiro, como o do Sistema Único de Saúde (SUS), o que indicaria um possível acesso ou vazamento por parte de fontes estatais. São fornecidos detalhes sobre o tipo de dose (primeira ou segunda), o nome da vacina administrada, o número do lote, o fabricante, a data exata da aplicação e o estabelecimento de saúde onde foi administrada (ver Imagem 4). Além de constituir uma grave violação de privacidade, esse tipo de informação pode ser usado para diversos fins indevidos, incluindo a falsificação de atestados médicos ou o roubo de identidade para acesso a serviços médicos.

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

Imagem 4. Evidências visuais da venda de dados relacionados ao histórico de vacinação.



Além do comando /**cpf**, que exige o número de identificação da pessoa, os *bots* também permitem executar o comando **/nome**, ou seja, pesquisar registros de dados pessoais de alguém à venda usando o nome e sobrenome, sem precisar saber o **CPF**. O *bot* responde com uma lista de correspondências que inclui nome completo, número do **CPF**, gênero e data de nascimento.

Nos grupos investigados, também é possível consultar dados pessoais utilizando números de telefones celulares e placas de veículos. Além disso, o comando **/cnpj** permite o acesso a informações detalhadas sobre pessoas jurídicas (empresas, fundações ou associações) utilizando o seu número de identificação fiscal. A consulta devolve uma ficha com dados como a razão social (nome legal da empresa), o nome comercial, a natureza jurídica (associação civil, sociedade anônima ou cooperativa), a situação atual da empresa ("ativa" ou "inativa"), a data de abertura, o capital social declarado e o porte da empresa, categorizado de acordo com seu tamanho (micro, pequena, média, etc.).

4.1.1 Contexto tecnopolítico e legal

Segundo a empresa global de cibersegurança Surfshark, em 2024, o Brasil ocupou o sétimo lugar no mundo em vazamentos de dados[26]. Isso demonstra que os incidentes de vazamento não são nem algo novo nem raro no país e podem ter contribuído para alimentar e viabilizar o mercado ilegal de informações pessoais. Um dos casos mais emblemáticos de vazamento de informações ocorreu em 2021, quando dados de mais de 223 milhões de pessoas foram expostos, incluindo número do **CPF**, nome, data de nascimento e gênero. O número ultrapassa a população total do Brasil, indicando que os registros de pessoas falecidas também foram comprometidos[27].

A magnitude dos vazamentos no Brasil deve ser analisada considerando um ecossistema digital caracterizado pelo uso massivo de aplicativos de mensagens e redes sociais[28], assim como por altos índices de fraude e criminalidade digital. Segundo dados do Senado Federal, um em cada quatro brasileiros com mais de 16 anos relatou ter sido vítima de um ataque cibernético em 2023[29], e estudos recentes estimam perdas anuais superiores a 70 bilhões de reais (equivalente a quase 13 bilhões de dólares em outubro de 2025) devido a fraudes financeiras e roubo de dados de cidadãos brasileiros[30]. Este contexto combina uma penetração tecnológica muito elevada com baixos níveis de alfabetização digital e uma crescente sofisticação dos mecanismos de fraude e roubo de identidade[31].

Nesse contexto, o uso do Telegram -um dos aplicativos mais populares do país- tem sido acompanhado de tensões com instituições nacionais em relação à circulação de informações ilícitas e ao descumprimento de decisões judiciais. Em março de 2022, o Supremo Tribunal Federal (STF) ordenou a suspensão temporária da plataforma devido à falta de cooperação com o sistema judicial.[32]. A medida foi revertida dois dias depois, após a empresa se comprometer a nomear um representante legal no país, cumprir as ordens judiciais e estabelecer mecanismos de cooperação com o Tribunal Superior Eleitoral (TSE)[33].

26. Para mais informação, 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. Disponível em: **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. Disponível em: **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. Disponível em: **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. Disponível em: **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? Disponível em: **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. Disponível em: **https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=483659&ori=1**

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

Diante desse cenário de vazamentos de dados e riscos crescentes, é crucial considerar o atual marco regulatório vigente no Brasil. O país conta com a Lei n. 13.709 - Lei Geral de Proteção de Dados Pessoais (LGPD), promulgada em 2018 e em vigor desde 2020.[34] A LGPD regula o tratamento de dados pessoais, inclusive em meios digitais, por pessoas físicas e jurídicas, públicas ou privadas, com o objetivo de proteger os direitos fundamentais à liberdade, à privacidade e ao livre desenvolvimento da personalidade. Entre seus princípios figuram a segurança, a prevenção e a não discriminação.

A LGPD define dados sensíveis como aqueles relacionados à "origem racial ou étnica, crença religiosa, opinião política, filiação sindical, saúde, vida sexual, dados genéticos ou biométricos vinculados a uma pessoa". Considerando essa definição, informação como os históricos de vacinação -que circulam nos mercados ilegais do Telegram- constitui informação sensível. Os regulamentos estabelecem obrigações mais rigorosas para esses casos, incluindo medidas específicas de segurança da informação.

A lei também dedica um capítulo ao tratamento de dados por entidades públicas, embora sem estabelecer regras muito diferenciadas ou rigorosas. Entre as suas disposições mais relevantes está a possibilidade de, em casos de infrações cometidas por entidades estatais, a Agência Nacional de Proteção de Dados (ANPD) emitir recomendações com o objetivo de cessar a violação. Isso indicaria que, se fosse encontrada alguma ligação entre a circulação indevida de dados pessoais em grupos do Telegram e a responsabilidade do Estado no tratamento ou proteção desses dados, o órgão teria o poder de intervir em nível administrativo para mitigar os danos e promover medidas específicas de reparação para o caso.

A ANPD foi criada em 2019, inicialmente sob a estrutura da Presidência da República, sem efetiva independência[35]. Em 2022, adquiriu caráter de autonomia especial, passando a estar vinculada ao Ministério da Justiça e Segurança Pública. No entanto, continuou a enfrentar limitações em termos de recursos humanos e financeiros[36] e sua atuação sancionadora tem sido tímida até o momento. Muito recentemente, em setembro de 2025, com a Medida Provisoria 1.317/2025[37], a ANPD foi transformada oficialmente em agência reguladora, deixando de estar subordinada ao Ministério e obtendo total autonomia técnica, funcional, administrativa e decisória. Essa reforma institucional também criou novos cargos especializados e fortaleceu sua capacidade operacional, o que pode ampliar seu escopo de atuação futura diante de intervenções estatais em casos de tratamento inadequado de dados.

Em paralelo, o Código Penal brasileiro criminaliza a invasão de dispositivos informáticos desde 2012, com penas de 1 a 4 anos de prisão e multa. As penas para o crime são agravadas quando resultam na obtenção e comercialização de dados,

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

35. Para mais informação, 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. Disponível em: **https://telesintese.com.br/em-aniversario-de-3-anos-anpd-reivindica-estrutura-proporcional-ao-desafio/**

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

especialmente se envolverem entidades públicas ou serviços financeiros, situações que podem estar relacionadas com as práticas descritas neste relatório.[38]

Em matéria de cibersegurança, o Brasil adotou em agosto de 2025 a nova Estratégia Nacional de Cibersegurança (E-Ciber), que atualiza a anterior de 2020.[39] A estratégia está estruturada sob os projetos temáticos de proteção e conscientização da cidadania; segurança e resiliência dos serviços essenciais e infraestruturas críticas; cooperação e integração entre órgãos e entidades públicas e privadas; e soberania nacional e governança. Entre as ações previstas está incluído o incentivo à expansão dos serviços de apoio às vítimas de crimes ilícitos em espaços digitais.

Em 2023, ainda sob a vigilância da Estratégia anterior, foi criado o Comitê Nacional de Cibersegurança (CNCiber). Este órgão colegiado, presidido pelo Gabinete de Segurança Institucional da Presidência da República, reúne representantes do governo, da academia, do setor privado e da sociedade civil. Seu mandato inclui propor atualizações na estratégia, formular medidas para prevenir e responder a incidentes e promover a cooperação internacional em relação ao tema.[40]

Em síntese, o Brasil conta com uma arquitetura legal e institucional relativamente robusta, que inclui uma lei moderna de proteção de dados, um marco penal específico para delitos informáticos e uma estratégia nacional de cibersegurança. No entanto, a escassa cultura de proteção de dados e de cibersegurança, somada à capacidade limitada operativa da ANPD e sua recente independência, reduzem a efetividade dos marcos vigentes. Num país de dimensões continentais, marcado por um histórico recorrente de vazamentos massivos e fraudes digitais, os riscos para a cidadania aumentam.

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

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

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

4.2 Peru

No Peru, oito grupos e dois canais de Telegram foram analisados. Os grupos apresentam um alcance amplo em relação à extensão do país, enquanto os canais têm uma base de assinantes muito menor:

Tabela 3. Número de assinantes dos canais 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

Assim como no Brasil, foram identificados *bots* com funções de administração, encarregados de responder consultas ou executar pesquisas. Paralelamente, os administradores humanos parecem manter estruturas hierárquicas com denominações como "owner", "*founder*", "*admin*", "*moderador*" ou "*dev*", replicando o esquema funcional de muitas comunidades digitais formais.

Um elemento socialmente significativo observado em alguns grupos foi o uso de linguagem discriminatória nas funções atribuídas, com nomes como "Gato Gay" ou "Cabro" (térmo pejorativo na gíria local) atribuídos a contas administradoras. Essas denominações refletem um imaginário marcado por lógicas machistas, LGBTQIA+-fóbicas e excludentes em geral, comuns em ambientes altamente masculinizados, que normalizam a burla a respeito de identidades diversas. Sua presença revela que, além da estrutura técnica, esses espaços também reproduzem dinâmicas sociais de discriminação baseadas em gênero e orientação sexual.

O modelo de negócio predominante no Peru também é o *freemium*, embora com algumas diferenças em relação ao Brasil. Em alguns grupos, o *bot* permite realizar pesquisas gratuitas, mas os resultados aparecem parcialmente ocultos: são exibidos nomes e títulos, enquanto o resto dos dados pessoais (como data de nascimento, direção e idade) aparecem substituídos por asteriscos (***). Para desbloquear essas informações, o *bot* sugere a compra de créditos. Esse modelo gera una experiência de "prova parcial" que motiva a compra.

A maioria dos grupos opera sob uma lógica de cobrança por funcionalidade -por exemplo, com funções básicas e funções Pro ou VIP-, ainda que tenham sido encontrados planos baseados em períodos de tempo (por dias ou meses). Os preços oscilam entre 2,20 dólares por acesso de três dias até montes anuais de 116,20 dólares, sendo este o último um dos valores mais altos registrados em toda a pesquisa. Além disso, existem pacotes que oferecem créditos, o que permite acumular saldo virtual para consultas específicas. A apresentação de planos em níveis (Básico, Padrão e Premium) sugere uma estratégia de escalonamento de benefícios vinculada ao pagamento, em uma lógica semelhante às plataformas legítimas de serviços digitais.

Os métodos de pagamento mais comuns são as carteiras digitais Yape e Plin, amplamente utilizadas a nível nacional no Peru. Ambas plataformas permitem enviar

dinheiro penas com um número de celular ou um código QR, sem necessidade de conhecer o nome ou número de conta bancária da pessoa destinatária. Se por um lado essas faturas digitais permitem um certo nível de rastreamento, já que o nome completo do titular aparece no momento da realização da transferência, seu uso continua sendo frequente nos mercados ilegais observados.

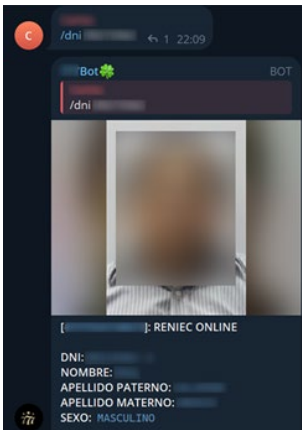
O comando mais comum para consultar e comprar dados em grupos e canais peruanos é /**dni**, que permite acessar uma grande variedade de dados de qualquer pessoa cidadã a partir de seu Documento Nacional de Identidade (DNI). O DNI é o número único de identificação designado a cada persona no Peru pela Reniec[41], que atua como entidade oficial encargada.

Após esse tipo de consulta, observou-se que os *bots* geravam em segundos uma resposta automática com uma ficha de dados pessoais detalhados, que só deveriam ser encontrados nos registros oficiais. Isso sugere um possível acesso indevido a bases de dados do Estado ou a filtragem desses registros por parte de atores maliciosos. A resposta inclui nomes completos (nome, nome paterno e materno), sexo e data de nascimento. Além disso, estão incluídos dados sobre o local de nascimento, como departamento, província e distrito.

Outros campos revelam detalhes adicionais como o estado civil, o grau de instrução, a estatura, e diversas datas importantes: inscrição, emissão, validade do DNI e em alguns casos até a data de falecimento da pessoa. Também mostra se a pessoa é doadora de órgãos. Em nível familiar, se listam os nomes e números de DNI do pai e da mãe. O sistema também fornece informações completas sobre o domicílio registrado, incluindo departamento, província, distrito e endereço.

Diferente do Brasil, a resposta automática inclui dados biométricos como impressões digitais das pessoas, aumentando exponencialmente o nível de exposição e vulnerabilidade dos direitos afetados. Em alguns casos, a fotografia também é acompanhada da assinatura manuscrita das pessoas (ver Imagem 5).

Imagem 5. Evidência visual sobre venda de dados através do comando /**dni**



41. Registro Nacional de Identificação e Estado Civil (Reniec): organismo autônomo do Estado peruano encarregado da identificação de pessoas naturais, da emissão do Documento Nacional de Identidade (DNI) e do gerenciamento do registro civil. Administra uma das principais bases de dados pessoais do país, incluindo nomes, datas de nascimento, domicílios e dados biométricos.

Além disso, observou-se que os *bots* nos grupos e canais peruanos também permitem obter imagens completas do DNI, tanto no formato eletrônico quanto na versão física ou virtual; até de crianças e adolescentes. Para isso, use comandos como / **dniel** para o DNI eletrônico (DNIe) e /**dniv** ou /**dnivir** para o DNI azul ou virtual, recebendo arquivos digitais em formato de imagem (.jpg ou .png) com a frente e o verso do documento. No caso do comando **/dniel**, os resultados mostram o DNI eletrônico completo de uma pessoa adulta, que conta com um chip integrado e é utilizado, entre outras coisas, para firmar documentos digitalmente.

É especialmente preocupante a qualidade dos documentos baixados observados, sendo suficientemente alta para utilização em falsificações, clonagem de identidade, acesso a serviços bancários ou qualquer tráfego digital. Além dos dados biométricos, o documento inclui informações detalhadas (como nomes, sobrenomes, sexo, data e local de nascimento), grau de instrução, estado civil, estatura, nome do pai e/ou mãe, endereço completa e situação de registro.

Em alguns casos, as fotografias e fichas de dados apresentam distintivos de órgãos oficiais do Estado peruano. Ainda não é possível determinar com certeza a origem dos dados comercializados, a presença de marcas, formatos e codificações coincidentes com os usados por entidades públicas gera alarmes sobre um possível acesso indevido a bases de dados oficiais ou à vazamento de documentos processuais. Um indício particularmente relevante aparece nas fichas de tipo C4[42], em que figura um apartado intitulado "Informações da consulta", que detalha quem realizou a pesquisa (nome do usuário), de qual entidade e com qual número da transação. Esse tipo de registro aponta para a possibilidade de que, em alguns casos, os *bots* empregados nos grupos do Telegram possam estar operando com credenciais institucionais válidas, o que permitiria realizar consultas diretas a sistemas oficiais e extrair dados em tempo real para sua posterior venda.

Também foi identificada a utilização de outros comandos que permitem o acesso a dados pessoais sem a necessidade de conhecer o número de identificação do proprietário; por exemplo, através do nome, da placa do veículo ou do número de telefone celular. Em relação a este último mecanismo de consulta, os dados são apresentados sob a etiqueta "OSIPTEL DATABASE - CEL". É importante ressaltar que o Órgão Supervisor de Investimentos Privados em Telecomunicações (OSIPTEL) é a entidade estatal responsável pela regulamentação e supervisão dos serviços de telecomunicações no Peru, incluindo o registro de linhas móveis associadas a pessoas físicas ou jurídicas.

Outros comandos identificados nos *bots* fueron **/hogar** [lar] e **/ag**, que permitem acesso a redes completas de vínculos familiares. Ao inserir o número do DNI no comando /**hogar**, o *bot* fornece informações sobre o endereço cadastrado, a situação econômica da família, sua classificação socioeconômica ("extremamente pobre", "pobre" ou "não pobre", de acordo com a classificação do Sistema de Focalización de Hogares - SISFOH, no Peru), detalhes sobre se está em uma área rural ou urbana, bem como os dados de cada um dos membros da unidade familiar: nomes, sobrenomes, DNI e data de nascimento.

42. O certificado C4 contém informação básica do DNI de uma pessoa. Trata-se de um certificado informativo, que não substitui o documento de identidade (DNI), mas é utilizado como medida de segurança para verificar a identidade em alguns serviços digitais. Disponível em: **https://www.gob.pe/8803-solicitar-certificado-de-inscripcion-c4**

Por fim, a pesquisa também revelou a venda do que parecem ser certidões oficiais de antecedentes criminais policiais e judiciais, documentos que, em circunstâncias normais, só poderiam ser emitidos por meio de procedimentos formais (com preço e prazo de emissão) perante o Ministério do Interior (PNP) ou o Poder Judiciário do Peru. Em ambos os casos, os *bots* geram arquivos em formato PDF, supostamente emitidos pela Polícia Nacional do Peru e pelo Poder Judiciário Nacional, respectivamente. Os documentos incluem dados como imagem facial, nome completo, assinatura digital, número do documento, nacionalidade e o resultado da verificação se a pessoa possui condenações ou antecedentes criminais (ver Imagem 6).

Imagem 6. Evidência visual da venda de dados com certificados oficiais de antecedentes policiais e judiciais.

O acesso imediato a esses certificados, sem passar pelo processo oficial de solicitação que normalmente exige autenticação, pagamento de uma taxa e um tempo de espera de horas ou dias, levanta questões sobre sua possível origem e sobre possíveis violações das plataformas estatais de emissão digital. Em alguns casos, os certificados foram gerados na mesma data e hora da consulta feita ao *bot* no Telegram, como mostra a Imagem 6, o que levanta a questão se esses sistemas poderiam estar diretamente vinculados, de forma não autorizada, a bancos de dados oficiais, ou se trata-se de uma simulação tecnicamente avançada de formatos institucionais.

A coincidência temporal entre o pedido e a emissão, juntamente com a fidelidade dos formatos, pode indicar a hipótese de que o acesso não provém de uma base de dados estática filtrada, mas sim de uma interação direta com os sistemas oficiais. No entanto, na ausência de provas conclusivas, ambos os cenários permanecem em aberto e requerem verificação técnica adicional.

4.2.1 Contexto tecnopolítico e legal

No Peru, assim como em outros países da região, vazamentos massivos de dados pessoais são um fenômeno recorrente que afeta tanto instituições públicas quanto privadas.[43] Em junho de 2025, a Autoridade Nacional Peruana de Proteção de Dados Pessoais (ANPDP) emitiu um alerta urgente após um vazamento que expôs 16 bilhões de senhas vinculadas a serviços como Apple, Google e Facebook, instando os cidadãos a alterarem suas senhas imediatamente para reduzir o risco de fraude e roubo de identidade[44].

Esse cenário geral também se reflete no uso de aplicativos de mensagens, nos quais foram documentados incidentes que mostram como vazamentos podem alimentar diretamente o mercado ilegal de dados. En 2024, durante a emissão de uma reportagem televisiva[45], jornalistas foram ameaçados via WhatsApp por indivíduos mal-intencionados que lhes enviaram dados pessoais obtidos no Telegram. As ameaças consistiam no envio de fichas da RENIEC com dados completos dos jornalistas, acompanhadas de mensagens intimidatórias. Ao exibirem seu acesso a essas informações pessoais, os responsáveis buscaram incitar o medo e demonstrar suas capacidades de rastreamento. A mesma reportagem televisiva revelou que os dados desses jornalistas estavam disponíveis em grupos do Telegram, como os analisados nesta pesquisa, nos quais basta inserir um número de documento para acessar os dados pessoais de qualquer pessoa[46].

Meses depois, ainda em 2024, outro incidente grave foi relatado no Peru: os dados de mais de 3 milhões de clientes do Interbank foram roubados e publicados na *dark web*. Segundo a cobertura jornalística do caso[47], um usuário anunciou que esses dados podiam "ser obtidos" via Telegram, sem que a reportagem tenha verificado sua comercialização efetiva em tal plataforma. Além do alerta, a cobertura fornece um elemento técnico relevante para a análise. Os arquivos relacionados ao caso contêm um script que descreve o acesso a um banco de dados hospedado no New Relic (provedor do Interbank) usando credenciais (nome de usuário e senha), e revela conhecimento de detalhes internos da estrutura do servidor que se tentava ter acesso[48]. Esses indícios não constituem prova conclusiva da rota de vazamento, mas reforçam a hipótese de acesso com informações interna ou uma configuração de segurança vulnerável, e ajudam a explicar como vazamentos dessa magnitude podem alimentar, direta ou indiretamente, circuitos de dados ilegais em mensagens e fóruns.

43. Cuzcano, X. (2025). Filtraciones de datos: el costo ciudadano de la negligencia digital. Disponível em: **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. Disponível em: **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. Disponível em: **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. Disponível em: **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'? Disponível em: **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/**

Em termos regulatórios, o marco de proteção de dados em vigor no Peru existe há mais de uma década. Está definida pela Lei n. 29733 - Lei de Proteção de Dados Pessoais, promulgada em 2011, cujo objetivo é garantir o direito fundamental à proteção de dados pessoais reconhecido na Constituição[49]. A norma considera como dados sensíveis aqueles que incluem informações biométrica, renda econômica, opiniões políticas, convicções religiosas, filosóficas ou morais, filiação sindical, bem como informações relacionadas à saúde ou à vida sexual; categorias que correspondem a vários dos tipos de dados identificados como sujeitos à comercialização nesta pesquisa.

Entre os princípios orientadores da lei está a segurança, que obriga os responsáveis pelas atividades de tratamento a implementar medidas técnicas, organizacionais e legais para evitar acessos não autorizados e garantir a integridade dos dados. Assim, a norma reconhece expressamente o direito das pessoas titulares de serem indenizados quando um tratamento indevido de dados lhes causar danos.

Em novembro de 2024 se aprovou uma nova regulamentação da Lei de Proteção de Dados Pessoais[50] no Peru, que introduz avanços relevantes, como a obrigação de comunicar incidentes de segurança à ANPDP, a exigência de políticas de segurança documentadas e a implementação de controlos de acesso mais rigorosos. Embora essas reformas busquem fortalecer a proteção dos titulares dos dados, a ausência de regras diferenciadas para agentes públicos de tratamento de dados continua sendo uma limitação fundamental da lei.

Essa falta de especificidade é relevante porque as entidades estatais gerenciam grandes volumes de dados -incluindo dados sensíveis- o que amplifica o impacto potencial de qualquer vazamento ou uso indevido. Sem critérios mais rigorosos de segurança, transparência e responsabilização aplicáveis ao setor público, a lei corre o risco de oferecer um nível desigual de proteção, deixando os cidadãos mais vulneráveis justamente diante daqueles que detêm os maiores repositórios de dados pessoais.

A aplicação da lei está a cargo da ANPDP, vinculada ao Ministério da Justiça e dos Direitos Humanos, por meio da Direção Nacional de Justiça[51]. A ANPDP possui poderes de sanção e coerção e, em teoria, independência para supervisionar tanto atores públicos quanto privados. No entanto, como está institucionalmente vinculada ao referido Ministério, essa autonomia pode ser limitada na prática, especialmente quando se trata de supervisionar entidades estatais ou impor sanções dentro da mesma esfera governamental.

Em paralelo, desde 2013 está vigente a Lei n. 30096 - Lei de Delitos Informáticos[52], que criminaliza condutas como o acesso ilegal a sistemas e a interceptação de dados informáticos, estabelecendo penas agravadas quando os atos envolvem informações classificadas ou afetam a defesa e a segurança nacional. Reformas recen-

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

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

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

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

tes, introduzidas por meio de decretos e acordos interinstitucionais, fortaleceram a coordenação entre a Polícia Nacional, o Ministério Público e órgãos especializados, criando unidades de combate ao cibercrime e protocolos de troca de informações. Além disso, foram incorporadas obrigações de formação técnica para funcionários e autoridades judiciais na área de pesquisa digital.

Por fim, na área de cibersegurança, o Peru desenvolveu a Estratégia Nacional de Segurança e Confiança Digital 2021-2026[53], cujos pilares incluem a promoção de uma cultura de segurança, a proteção de ativos críticos, o desenvolvimento de capacidades e a prestação de serviços digitais. O documento, no entanto, não foi adotado formalmente como política de Estado[54]. Essa omissão limita sua força normativa e proativa e reflete a fragilidade institucional para articular respostas eficazes em questões de segurança cibernética. Essa falta de implementação também evidencia a desconexão entre as políticas de cibersegurança e as políticas de proteção de dados pessoais, que, na prática, deveriam ser abordadas em conjunto como dimensões complementares da segurança e da confiança digitais.

Nos desafios da pesquisa, essa fragilidade institucional se manifesta na ampla circulação de dados pessoais e de documentos que parecem reproduzir o formato ou os atributos dos emitidos por entidades públicas. Embora não seja possível determinar com certeza sua origem, a semelhança com registros oficiais sugere deficiências nos controles de segurança e na supervisão sobre o tratamento de dados, inclusive de dados sensíveis.

53. Disponível em: **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. Disponível em: **https://www.derechosdigitales.org/wp-content/uploads/DD_CYRILLA_ESP_2024.pdf**

4.3 Argentina

Na Argentina foram identificados seis canais e um grupo, com um modelo de operação distinto do observado no Brasil e no Peru. Nesse caso, o esquema prioriza a comunicação direta e discreta entre vendedores e compradores. Observou-se que os canais funcionam como ponto de entrada: ali se difundem anúncios, planos e evidências de venda, ao passo que as transações são concretizadas de maneira personalizada por meio de chats um a um. O alcance dos espaços investigados é o seguinte:

Tabela 4. Número de assinantes dos canais observados

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

Como predominam os canais sobre os grupos, a visibilidade das figuras administradoras muda, pois nos canais do Telegram não é possível ter acesso à lista de assinantes nem identificar quem gerencia o espaço, o que dificulta a compreensão de como se estrutura.

Foi identificado que o modelo na Argentina é muito mais centralizado em vendedores humanos. Assim, em vez de permitir pesquisas gratuitas ou interações autônomas com *bots* do grupo, as operações são canalizadas através do chat privado entre cliente e vendedor. Uma vez iniciado o contato, o vendedor envia os preços e meios de pagamento disponíveis e logo após a transação se concretizar, o *bot* é adicionado e ativado nesse mesmo chat privado. Esse funcionamento pode ser observado a partir das referências que os próprios vendedores publicam nos canais abertos, nos quais explicam o modo de operação e os passos que devem seguir as pessoas interessadas. A estratégia empreendida elimina por completo as buscas gratuitas ou parciais e se estabelece como regra que todo o processo é pago, com base em uma lógica de trato personalizada que simula uma "atenção direta ao cliente".

Nessa linha, os vendedores geralmente oferecem diferentes "planos" dependendo do tipo e volume de informações necessárias. Em alguns casos, o modelo inclui acessos temporais, ou seja, permissões de uso limitadas por um período determinado (como horas ou dias) durante o qual o comprador pode realizar consultas e, em certos casos, baixar os resultados. Em outros casos, são comercializados pacotes por volume de buscas, que restringem a quantidade de dados obtidos em função do valor do pagamento realizado. O esquema de preços é mais orientado ao uso de tokens como moeda interna, entendido como unidades virtuais de pagamento que são adquiridas previamente e depois consumidas dentro do *bot* para habilitar funções ou consultas específicas. Este sistema rejeita um modelo transacional imediato, no qual a pessoa usuária compra apenas o que precisa.

Foram identificados pacotes que oferecem acesso a partir de 3,5 dólares por dia -com uso do *bot* habilitado somente por 24 horas- até serviços "permanentes" por 15 dólares, que outorgam acesso contínuo sem limite de tempo. Também é possível encontrar modalidades baseadas em tokens, como a venda de 1000 unidades por 100 dólares, em que cada token equivale a uma consulta ou uma função habilitada dentro do *bot*. O método mais utilizado é Mercado Pago, plataforma digital de paga-

mentos desenvolvida por Mercado Livre. Essa ferramenta se converteu em uma das mais populares da Argentina (e toda América Latina)[55] para transações eletrônicas.

Diferente entre os sistemas de pagamento predominantemente usados no Brasil e no Peru (que funcionam, respectivamente, como mecanismos de pagamento instantâneo entre pessoas e boletos digitais), Mercado Pago opera como intermediário financeiro dentro de uma plataforma comercial, gerenciando contas de usuários e oferecendo maior formalidade nas transações. No entanto, seu uso por vendedores nos canais ilícitos sugere que, apesar de sua estrutura empresarial e rastreabilidade potencial, também pode ser aproveitado para operações desse tipo. Na prática, no momento de realizar o pagamento, é visualizado o nome da pessoa ou empresa receptora, o que indica que, assim como nos casos dos outros países investigados, não se trata de um sistema completamente anônimo, embora sua intermediação introduza um nível diferente de opacidade operativa.

No entanto, alguns espaços analisados também migraram para o uso de criptomoedas, o que representa um nível maior de encobrimento transacional e menor rastreabilidade, em consonância com práticas comuns em mercados ilícitos globais[56]. Esta diversidade de meios de pagamento responde às restrições locais, como os controles bancários e os limites para o envio de dinheiro vivo ou digital e sugere a necessidade dos vendedores de evadir a rastreabilidade das transações através do sistema financeiro formal.

A presença de registros de compras anteriores e respostas automáticas compartilhadas como "demonstração" em canais públicos observados -isto é, exemplos de consultas reais compartilhados pelos vendedores para mostrar que o serviço funciona (chamadas "referências")- evidencia que não se trata de transações isoladas. Pelo contrário, a repetição desses exemplos indica um fluxo contínuo de aquisição de dados, refletindo a regularidade com que esses mercados digitais estão sendo utilizados.

Em diversos exemplos identificados, os *bots* retornam resultados que incluem dados supostamente obtidos do Cadastro Nacional de Pessoas (Renaper), entidade responsável pelo banco de dados de identidade na Argentina. Essa inferência é corroborada tanto pelo fato de que tais dados (fotografia, número do documento, afiliação e outros) só deveriam ser registrados no Renaper, quanto pelo fato de alguns dos arquivos analisados apresentarem formatos e marcas que coincidem com os utilizados oficialmente por essa instituição. Entre esses elementos está a presença de um código chamado "IDARG" pelos *bots*, um identificador alfanumérico incluído no documento de identidade eletrônico argentino e usado para validar a autenticidade do documento.

Um dos comandos mais usados nos canais argentinos é /**dni**, que, dentro dos pacotes pagos oferecidos pelos vendedores, permite o acesso a informações detalhadas sobre qualquer pessoa, bastando inserir o número do seu documento de identida-

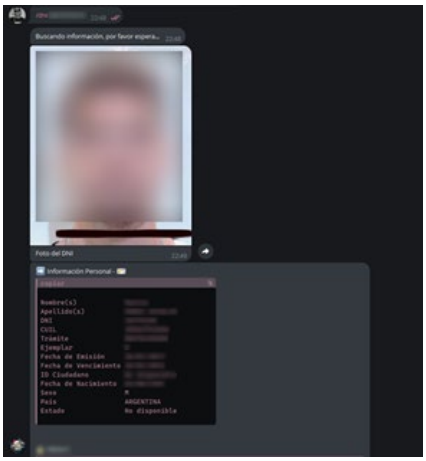
55. Para mais informação, ver: **https://paymentscmi.com/insights/metodos-pagamento-mais-utilizados-america-latina-brasil-mexico-chile-peru-colombia-argentina/**

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

de nacional. Assim como no Peru, a resposta do *bot* inclui a imagem facial oficial extraída do documento e, em alguns casos, sua assinatura digitalizada.

Em diversos canais, essas imagens compartilham um padrão visual: recursos de segurança e marcas d'água institucionais, ou seja, elementos gráficos comumente usados para autenticar documentos oficiais e prevenir sua falsificação, como selos digitais, fundos padronizados ou escudos em relevo. Há casos de fotografias com inscrições de entidades como escolas e ministérios específicos, o que sugere vazamentos de dados que podem vir de sistemas internos dessas instituições escolares e da administração pública (ver Imagem 7).

Imagem 7. Evidência visual sobre venda de dados através do comando /**dni**



Particularmente alarmante é um caso em que a imagem de um adolescente é exibida, juntamente com dados como nome, número de identificação e data de nascimento, com uma marca d'água que indica "Sistema Federal de Comunicações Policiais" (SIFCOP). Esse sistema é uma ferramenta oficial restrita, utilizada exclusivamente para a troca de informações de interesse criminal entre as forças policiais e os órgãos judiciais[57]. Seu acesso está regulado por protocolos estritos, o que agrava o potencial vazamento ocorrido.

Além disso, os *bots* fornecem um formulário estruturado com dados como nome completo, número de identificação, CUIL (Código Único de Identificação Laboral, equivalente ao CNPJ), número da transação, número da cópia, data de emissão e validade do documento, nacionalidade, sexo, data de nascimento e situação cadastral, que pode incluir certidão de óbito.

Essas informações são complementadas pelo endereço completo da pessoa: rua, número, bairro, código postal, cidade, município, província e até mesmo andar ou bloco de prédio (monoblock)[58]. Em alguns casos, a resposta inclui um link direto para o Google Maps, o que facilita a geolocalização do endereço, aumentando significativamente o risco de práticas como rastreamento, vigilância privada, assédio

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

58. Na Argentina, um "monoblock" é um bloco de apartamentos dentro de um complexo habitacional, geralmente parte de edifícios estatais ou de habitações sociais. Geralmente, é identificado junto com o andar e número da unidade para localizar com precisão um endereço em complexos de edifícios.

ou sequestro. A consulta também inclui informações detalhadas contidas na carteira de habilitação da pessoa que possui o DNI (como número, categoria e datas de emissão e validade).

Em alguns locais, também é possível acessar informações financeiras detalhadas de pessoas através do comando **/nosis** seguido pelo CUIT (Código Único de Identificação Fiscal) ou número de DNI. Este comando parece se referir ao banco de dados do sistema de crédito "NOSIS", uma das plataformas mais conhecidas na Argentina para relatórios de risco financeiro e de crédito.[59]

Após esse comando, em primeiro lugar, o *bot* mostra informação pessoal básica. O relatório detalha então a situação profissional da pessoa: se é empregadora, se pertence a uma sociedade, se está empregada ou trabalha de forma autônoma, e se teve conta bancária nos últimos meses. A antiguidade no base de dados da Administração Federal de Ingressos Públicos (Afip) também é indicada. Além disso, a situação de crédito da pessoa é avaliada (ver Imagem 8). A "pior situação" registrada é apresentada, juntamente com o número de bancos envolvidos, o valor total devido, o compromisso mensal (relação renda/dívida), a pontuação de crédito e sua evolução ao longo do tempo. Em outras palavras, essa seção fornece um retrato claro do comportamento financeiro da pessoa.

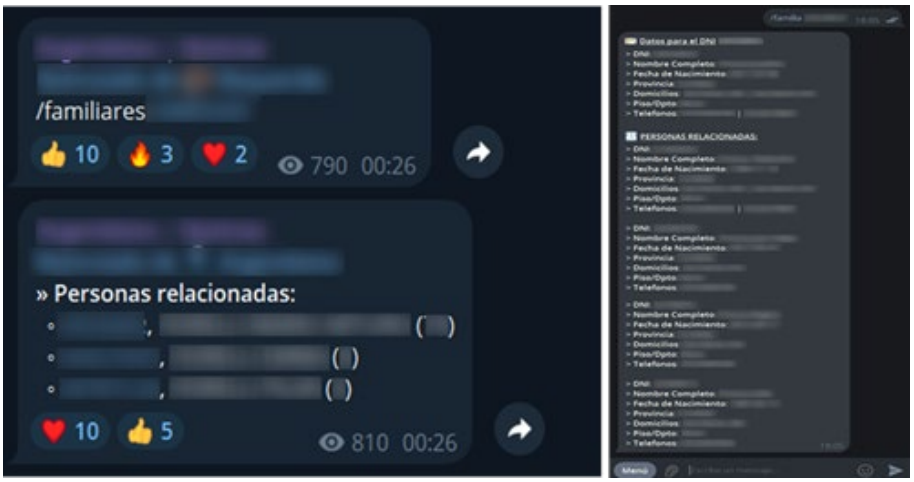
Imagem 8. Evidencia visual sobre venda de dados com informação da situação de crédito

59. "NOSIS foi fundada em 1988 com o objetivo de fornecer informações sobre o contexto empresarial, os mercados financeiros online e o comércio exterior, a fim de oferecer ferramentas analíticas que facilitem a tomada de decisões. Mais de 25.000 clientes comprovaram que nossos bancos de dados, tanto de fontes próprias quanto públicas, são os mais completos e atualizados do mercado". Disponível em: **https://www.nosis.com/es/institucional/quienes-somos**

O *bot* também revela campos técnicos do documento de identidade (como o código de barras e as linhas completas do sistema de leitura mecânica MRZ), elementos que não apenas validam o documento, mas também permitem sua clonagem ou replicação para fins maliciosos. Além disso, como já mencionado, um dos elementos técnicos mais alarmantes retornados pelo *bot* é o IDARG, um código alfanumérico presente no documento de identidade eletrônico argentino, usado para validar a autenticidade do documento. A inclusão deles nessas respostas indica acesso a camadas profundas do sistema de emissão de identidade do país.

Em alguns casos, o uso do mesmo comando de consulta, seja /dni, **/consulta** ou variantes, pode retornar informações ainda mais sensíveis e detalhadas, incluindo laços familiares de crianças e adolescentes, como filhos e filhas da pessoa procurada. Também se identificou o comando **/familia** ou **/familiares** seguido do número de DNI, por meio do qual o *bot* consegue retornar tanto os dados da pessoa consultada quanto os de seus familiares diretos, como se vê na Imagem 9. As respostas geradas incluem informações detalhadas, como nomes completos, datas de nascimento, endereço, província e, em vários casos, também os números de telefone associados a cada pessoa. Em alguns casos, inclusive é mostrada a idade atual dos familiares.

Imagem 9. Evidência visual sobre venda de dados através do comando **/familia**



Outros comandos de busca observados incluem nome, número de telefone e placa do veículo. As informações fornecidas incluem dados pessoais, endereço completo, contatos telefônicos com o nome da operadora, e-mails, laços familiares (com nomes, idades e parentesco) e até mesmo histórico profissional, com o nome da empresa, situação empregatícia e número CUIT (equivalente ao CNPJ) do empregador.

Finalmente, na Argentina, também se documentou a venda de informação vinculada a pessoas jurídicas. Utilizando o comando **/company** seguido de um número CUIT, os *bots* retornam dados detalhados sobre uma entidade oficialmente registrada no país.

4.3.1 Contexto tecnopolítico e legal

Assim como outros países da região, a Argentina tem um histórico de graves incidentes de segurança de dados. Em 2021, por exemplo, mais de 116 mil fotografias da Renaper foram compartilhadas indevidamente no Telegram. El episódio deu lugar a uma pesquisa judicial e à apertura de um relatório interno[60], embora nenhum resultado conclusivo sobre seu alcance ou sobre os possíveis responsáveis tenha sido publicado até setembro de 2025.

Naquele mesmo ano, outro ataque comprometeu o banco de dados público do sistema de carteiras de habilitação, colocando mais de 6 milhões de pessoas em risco[61]. Esses incidentes destacam a fragilidade dos mecanismos de segurança dos bancos de dados estatais e também mostram que o problema é anterior e transcende o uso do Telegram.

No entanto, é importante destacar que o país foi pioneiro na região em matéria regulatória: em 2000, promulgou a Lei n. 25.326 sobre a Proteção de Dados Pessoais[62], uma das primeiras da América Latina. A norma "tem por objeto a proteção integral dos dados pessoais contidos em arquivos, registros, bancos de dados ou outros meios técnicos de processamento de dados, sejam públicos ou privados, destinados a fornecer relatórios, a fim de garantir o direito à honra e à privacidade dos indivíduos, bem como o acesso às informações registradas sobre eles".

Estabelece direitos para os titulares dos dados, como acesso, retificação, eliminação, confidencialidade e atualização dos dados, e impõe obrigações de segurança da informação àqueles que os processam. No entanto, a lei não estabelece um regime diferenciado para agentes públicos, embora o Estado seja o principal responsável pela coleta e custódia dos dados dos cidadãos.

A aplicação da Lei n. 25.326 cabe à Agência de Acesso à Informação Pública (AAIP), uma autoridade criada em 2016[63], que é dependente da Chefatura de Gabinete de ministros. De acordo com o Artigo 29 da Lei de Proteção de Dados, entre as funções da Agência está monitorar o cumprimento das normas de segurança de dados e aplicar sanções administrativas em caso de descumprimento. No entanto, por estar inserida na própria estrutura do Poder Executivo, sua capacidade de monitorar violações originadas em agências estaduais pode ser limitada.

Em 2008, a Argentina fortaleceu seu arcabouço penal com a promulgação da Lei n. 26.388, que alterou o Código Penal e incorporou os crimes cibernéticos ao capítulo sobre "Violação de Segredos e Privacidade"[64]. Entre eles, o artigo 153 bis

60. Infobae (2024). Volvieron a publicar más de 116 mil fotos y números de DNI y pasaporte de argentinos robados al Renaper. Disponível em: **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. Disponível em: **https://www.vocescriticas.com/noticias/2024/04/03/156677-robaron-del-renaper-116-mil-fotos-de-ciudadanos-argentinos-para-venderlas-por-telegram**

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

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

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

pune com pena de prisão de quinze dias a seis meses o acesso ilegítimo a sistemas informáticos ou dados de acesso restrito, e agrava a pena quando envolve dados de entidades públicas ou prestadores de serviços financeiros. Da mesma forma, o Artigo 157 bis penaliza com pena de prisão de um a dois anos o acesso indevido a bancos de dados pessoais.

Na área de cibersegurança, em setembro de 2023, a Argentina aprovou sua Segunda Estratégia Nacional de Cibersegurança[65], um documento que, a primeira vista, representou um avanço significativo na região. A estratégia incluía, entre seus objetivos e diretrizes, princípios de direitos humanos, perspectiva de gênero, proteção de setores vulneráveis, cooperação internacional, soberania digital e salvaguarda de infraestruturas críticas. O estudo também considerou objetivos como o fortalecimento institucional, a proteção dos sistemas do setor público, a conscientização dos cidadãos e o desenvolvimento de um quadro regulatório alinhado aos novos desafios tecnológicos.

No entanto, esses avanços foram questionados após uma série de reformas recentes na governança da segurança cibernética.[66] Em julho de 2024, a reestruturação do Sistema Nacional de Inteligência dissolveu a Agência Federal de Inteligência e restaurou as funções da antiga Secretaria de Estado de Inteligência (SIDE), bem como da AAIP, sob o controle direto do Poder Executivo[67]. No ano seguinte, por meio do Decreto 274/2025, a SIDE assumiu o controle da Agência Federal de Cibersegurança, a implementação da Estratégia Nacional e a operação do **CERT.ar**[68]. Pouco tempo depois, em maio de 2025, a SIDE aprovou o Plano de Inteligência Nacional (PIN), declarado "secreto", ao qual apenas o presidente, a SIDE e uma comissão bicameral têm acesso.[69]. Segundo informações vazadas para a imprensa, esse plano concede poderes para coletar informações sobre pessoas que, na opinião do governo, "minam" a confiança pública em suas políticas[70], aprofundando as preocupações com a falta de transparência e controle democrático.

Nesse contexto, colocar a política de cibersegurança sob uma estrutura fechada de inteligência estatal, sem controles democráticos, implica que a estratégia nacional perde a independência e a capacidade de implementação eficaz. Em vez de garantir a proteção das pessoas e das infraestruturas críticas, conforme estabelecido pelos objetivos formais da Estratégia argentina, a falta de autonomia limita seriamente sua capacidade de resposta a violações como as documentadas nessa pesquisa, que apontam para um possível uso indevido de informações de bases de dados públicas e sua subsequente circulação no Telegram.

65. Disponível em: **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. Disponível em: **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. Disponível em: **https://defonline.com.ar/seguridad/dentro-de-la-side-asi-sera-la-agencia-federal-de-ciberseguridad/**

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

69. Para mais informação, 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. Disponível em: **https://www.lanacion.com.ar/politica/el-gobierno-niega-que-la-side-investigue-a-opositores-o-quienes-manipulen-la-opinion-publica-nid25052025/**

VOLTAR AO SUMÁRIO

5 TENDÊNCIAS REGIONAIS

Esta seção destaca três tendências que permeiam os resultados das pesquisas nacionais, relacionando-as a características específicas da América Latina como região. A primeira aponta para a possível origem de uma parcela significativa dos dados que circulam em grupos e canais do Telegram a partir de bases de dados públicas. Embora não seja possível confirmar isso de forma conclusiva, vários indícios (como formatos, codificações e referências institucionais) sugerem que algumas das informações podem ter sido obtidas por meio de raspagem de dados (*scraping*), vazamentos ou uso indevido de credenciais. Esse cenário revelaria não apenas limitações na aplicação das normas de proteção de dados, mas também fragilidades na segurança dos sistemas que armazenam e gerenciam informações pessoais, em um contexto de avanço acelerado das políticas de digitalização do Estado em países da América Latina. A segunda tendência está ligada ao gênero e mostra como o mercado ilegal de dados funciona como um insumo para a violência de gênero facilitada pela tecnologia, intensificando o controle, a extorsão e o silenciamento de mulheres e pessoas LGBTQIA+. Por fim, o terceiro ponto destaca a vulnerabilidade especial de crianças e adolescentes, agravada por práticas que os infantilizam e hipersexualizam em relação ao mercado ilegal de seus dados.

5.1 Indícios de origem pública dos dados e fragilidades na gestão da informação

Embora não seja possível determinar com certeza a origem dos dados comercializados nos grupos e canais analisados, diversos indícios sugerem que uma parte significativa das informações pode ter sido obtida de bancos de dados públicos ou registros oficiais. A coincidência no formato dos campos, na terminologia utilizada e na estrutura dos arquivos sugere a possível existência de vazamentos, acessos não autorizados ou uso indevido de informações estatais, o que representa sérios desafios em termos de segurança da informação e governança de dados, especialmente considerando as políticas de digitalização do Estado e dos serviços públicos que estão sendo intensificadas na América Latina.

Uma das pistas mais importantes sobre a possível origem de dados comercializados ilegalmente pode ser encontrada nos próprios espaços onde o uso de *bots* é promovido. Em alguns canais, especialmente na Argentina, os administradores reconhecem explicitamente que os dados provêm de técnicas de raspagem de dados (*scraping*) -uma técnica automatizada que permite extrair grandes volumes de dados de sites- o que nos permite inferir que as informações coletadas incluiriam dados de bancos de dados oficiais, com base na natureza dos registros e na presença de marcas d'água e formatos oficiais. O termo "scrap" aparece em mensagens disseminadas nesses canais

como uma habilidade técnica fundamental para acessar, coletar e, posteriormente, comercializar informações pessoais em larga escala. Nesse contexto, seria um processo pelo qual informações pessoais são coletadas sistematicamente de bancos de dados.

Além disso, algumas das evidências visuais analisadas apresentam estruturas de dados em formato JSON, um padrão amplamente utilizado para troca de informações entre sistemas, pois organiza os dados em pares "chave:valor". A identificação desse formato sugere que a informação pode ter sido extraída e processada diretamente de bases de dados ou sistemas automatizados, uma vez que sua estrutura uniforme e massiva é típica de ambientes digitais e não de compilações manuais. Também é mencionado que o robô é atualizado regularmente, o que exige um mecanismo de alimentação constante que dificilmente pode ser mantido manualmente.

Outro fator é que, no caso dos três países analisados, a identificação de dados cuja natureza e nível de detalhe coincide com aqueles que, em princípio, só deveriam ser encontrados em bases de dados públicos ou em registros administrativos do Estado. O histórico de vacinação ou de benefícios sociais no Brasil, as certidões de antecedentes criminais da polícia e do judiciário peruanos e os registros do Renaper na Argentina com o código Idarg são alguns dos exemplos mais relevantes.

A presença dessas informações nos ambientes de compra, venda e automação do Telegram pode refletir falhas estruturais nas arquiteturas legais e institucionais de proteção de dados e segurança cibernética na América Latina. Conforme mencionado, esse fenômeno ocorre em um contexto de digitalização acelerada das políticas e serviços públicos na região, impulsionada por estratégias estatais promovidas sob o argumento da eficiência[71]. No entanto, esse processo não foi acompanhado por padrões equivalentes de segurança, transparência e prestação de contas, inclusive em relação ao tratamento de dados pessoais envolvidos. A expansão das infraestruturas tecnológicas sem uma governança forte trouxe consigo riscos crescentes de exposição, vazamento ou reutilização indevida de informações estatais. Como mencionado anteriormente, embora não seja possível estabelecer uma relação direta, nos casos da Argentina, do Brasil e do Peru há indícios que apontam para vulnerabilidades ligadas a esses processos.

Nesse sentido, a venda de dados pessoais no Telegram pode estar ligada a uma fragilidade nas estruturas legais e institucionais de proteção de dados e segurança cibernética na América Latina. O ecossistema de extração automatizada e ilegítima de dados, que ocorre em flagrante desrespeito às normas de proteção de dados vigentes nos países analisados, transforma a identidade das pessoas em um insumo comercializável. Conforme apurou a pesquisa, com um único comando é possível ter acesso a informações que vão desde o rosto e o endereço exato até dados de saúde, financeiros ou vínculos familiares.

Tal debilidade regional tem ao menos três dimensões que requerem mais pesquisa para estabelecer suas origens, causas e respostas. A primeira é normativa. Embora a maioria dos países da região possua leis de proteção de dados e legislação sobre crimes cibernéticos, estas não são necessariamente suficientes no contexto da crescente digitalização, especialmente dos governos. As leis de proteção de dados rara-

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

mente estabelecem regimes diferenciados para o setor público, embora os Estados sejam os principais responsáveis pela coleta e custódia das informações dos cidadãos.

Em paralelo, a legislação sobre crimes cibernéticos oferece ferramentas criminosas cuja aplicação é limitada em comparação com a magnitude dos vazamentos e a sofisticação das redes criminosas. Além disso, no contexto latino-americano, em que os sistemas de justiça criminal enfrentam sérias deficiências estruturais (como sobrecarga e seletividade na acusação), o recurso ao direito penal é insuficiente e tem baixo potencial didático ou ressocializante, sendo potencialmente problemático como principal resposta a incidentes digitais. Embora a punição dos delitos cibernéticos tenha um valor social de reprovação desse tipo de conduta, focar a política institucional exclusiva ou principalmente na via punitiva deixa de lado dimensões chave como a prevenção, a educação digital, a reparação e o fortalecimento das capacidades institucionais.

Mesmo as estratégias nacionais de cibersegurança tendem a ser de curto alcance e geralmente apresentam sérias dificuldades para se traduzirem em políticas públicas eficazes. Como assinalamos em investigações recentes[72], a maioria das estratégias na América Latina não incorpora indicadores de conformidade ou abordagens de direitos humanos e de gênero, o que reduz significativamente seu impacto na proteção dos cidadãos no ambiente digital.

A segunda dimensão da fragilidade é institucional, relacionada à capacidade de fazer cumprir as leis. As autoridades de proteção de dados e os órgãos de cibersegurança frequentemente carecem de independência e/ou de recursos financeiros e humanos. Em muitos casos, fazem parte da mesma estrutura estatal que deveriam supervisionar, o que dificulta a pesquisa de vazamentos e a punição de violações cometidas por entidades públicas. No Brasil, a ANPD conquistou recentemente autonomia formal plena, mas ainda possui recursos limitados; no Peru, a autoridade depende diretamente do Ministério da Justiça e só recentemente reforçou sua regulamentação com obrigações de notificação e medidas de segurança; e na Argentina, a agência de proteção de dados se reporta ao Chefe de Gabinete, enquanto a política de segurança cibernética foi absorvida pelo sistema de inteligência, reforçando a opacidade e eliminando controles externos.

A existência de autoridades verdadeiramente independentes é um elemento central para garantir a proteção eficaz de dados pessoais e a segurança digital. Diversos organismos internacionais, entre eles a Organização para a Cooperação e o Desenvolvimento Econômico (OCDE)[73], enfatizam que a autonomia funcional, técnica e financeira dessas entidades é uma condição indispensável para garantir a responsabilização, especialmente do Estado, no tratamento das informações dos cidadãos. No contexto desta pesquisa, a falta de independência institucional traduz-se numa potencial impossibilidade prática de esclarecer a origem dos dados que circulam no Telegram ou de determinar eventuais responsabilidades públicas diante dos vazamentos. Sem capacidade ou recursos suficientes de fiscalização, as autoridades ficam relegadas a um papel reativo, o que perpetua um cenário de vulnerabilidade sistêmica na gestão

72. Derechos Digitales (2025). Ciberseguridad en América Latina: Estrategias nacionales en 2024. Disponível em: **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. Disponível em: **https://www.oecd.org/en/publications/governance-of-regulators-practices_9789264255388-en.html**

de informações estatais e baixa aplicação dos atuais marcos regulatórios.

Finalmente, a terceira dimensão da debilidade se vincula à segurança da informação nos próprios órgãos estatais. Embora as leis de proteção de dados na Argentina, no Brasil e no Peru reconheçam a importância de medidas de segurança adequadas e as estratégias nacionais de cibersegurança incluam a proteção de infraestruturas críticas e bases de dados públicas como prioridade, as evidências reunidas sugerem uma lacuna significativa entre o quadro regulamentar e a sua implementação prática. Na maioria dos casos, as instituições que concentram e administram grandes volumes de informações pessoais carecem de políticas abrangentes de gestão de riscos, auditorias técnicas regulares ou mecanismos de supervisão independentes.

Essa distância entre norma e prática cria vulnerabilidades que, embora nem sempre resultem em vazamentos verificáveis, ampliam as superfícies de exposição e os riscos de acesso indevidos, reutilização ou perda de informações sensíveis. Além do mais, os altos e históricos índices de vazamentos de dados na região[74] reforçam a ideia de que a América Latina carece de uma cultura sólida de segurança da informação, em que as medidas costumam ser reativas ou fragmentárias. Num contexto de crescente interconexão entre os sistemas estatais, a ausência de uma governança tecnológica eficaz enfraquece a capacidade dos Estados de resguardar a integridade dos dados que gerem e, simultaneamente, erosiona a confiança dos cidadãos nos processos públicos de digitalização.

A facilidade com que grupos e canais de compra e venda de dados operam no Telegram, juntamente com o potencial de extorsão ou roubo de identidade decorrente dessas práticas, destaca a magnitude dos riscos associados à má gestão de informações pessoais. Quando os dados expostos apresentam características compatíveis com registros gerenciados por entidades oficiais, o problema transcende a esfera individual e compromete a segurança coletiva e a confiança nas instituições públicas. Em conjunto, as conclusões desta pesquisa mostram que, apesar dos avanços regulatórios em proteção de dados e segurança cibernética, a região ainda enfrenta um déficit estrutural na capacidade de traduzir as regulamentações em garantias efetivas, o que mantém espaços de vulnerabilidade para os cidadãos.

5.2 O mercado ilegal de dados pessoais como insumo para a violência de gênero facilitada pelas tecnologias

A América Latina é uma das regiões mais desiguais do mundo, sendo a desigualdade de gênero uma de suas dimensões mais persistentes. Meninas e mulheres enfrentam níveis alarmantes de violência estrutural[75]. Segundo a Comissão Econômica para a América Latina e o Caribe (Cepal), pelo menos 4.050 mulheres foram vítimas de feminicídio em 2022 na América Latina e no Caribe, o que equivale a uma morte violenta de uma mulher em razão de seu gênero a cada duas horas[76]. Entretanto, o

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

75. Para mais informação, 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. Disponível em: **https://www.cepal.org/es/comunicados/2022-al-menos-4050-mujeres-fueron-victimas-femicidio-o-feminicidio-america-latina-caribe**

Mecanismo de Acompanhamento da Convenção de Belém do Pará (MESECVI), da Organização dos Estados Americanos (OEA), relata que entre 2018 e 2022 foram registrados mais de 802.000 casos de crimes sexuais contra mulheres, sendo quase 488.000 das vítimas meninas menores de 18 anos[77].

A população LGBTQIA+, por sua vez, enfrenta violações de seus direitos e segurança como consequência dos profundos níveis de desigualdade estrutural de gênero na região. O Brasil, por exemplo, lidera há anos os registros mundiais de assassinatos de pessoas trans e travestis. Em 2024, foram documentadas pelo menos 291 mortes de pessoas LGBTQIA+, representando um aumento de 13,2% em comparação com o ano anterior[78]. Esses números refletem a gravidade de uma violência de gênero profundamente enraizada e persistente, que encontra no espaço digital um novo terreno para reprodução e amplificação.

Neste contexto, a VGFT, definida como "qualquer ato de violência cometido, assistido ou agravado, total ou parcialmente, por meio de tecnologias de informação e comunicação contra uma pessoa em razão de seu gênero" (UNFPA)[79], deve ser entendida como uma continuidade da violência offline em direção aos entornos digitais. A VGFT abrange diversos comportamentos, incluindo o compartilhamento não consensual de imagens íntimas, o assédio cibernético, a manipulação de dados pessoais para extorsão e o controle coercitivo por meio de dispositivos e plataformas.[80] Mais que uma lista fechada, VGFT deve ser entendida como um fenômeno em constante evolução, marcado pela interação sociotécnica: não apenas a tecnologia avança, mas também as formas como ela é usada para exercer violência.

Além de observar grupos e canais de compra e venda de dados no Telegram, esta pesquisa incluiu uma pesquisa documental de publicações e depoimentos públicos em redes sociais que se referiam a essas dinâmicas. Nesse exercício, foram identificadas queixas específicas de pessoas que relataram ter sido vítimas de diferentes tipos de violência após a possível aquisição ou divulgação de seus dados pessoais por meio dessa plataforma. Esses casos nos permitem observar como a comercialização ilegal de informações pode estar ligada a práticas de intimidação, assédio e coerção, especialmente direcionadas contra mulheres e pessoas LGBTQIA+.

No Brasil, por exemplo, uma usuária relatou em suas redes sociais que um agressor havia obtido seus dados e os de sua mãe em um grupo do Telegram e os utilizado para extorqui-la sexualmente, exigindo vídeos íntimos sob ameaças explícitas. Da mesma forma, na Argentina foi documentado um caso em que a foto do DNI de uma mulher foi compartilhada em um grupo com comentários misóginos e homofóbicos, com o objetivo de expor seus dados pessoais (*doxxing*) e assediá-la. No Peru,

77. Para mais informação, ver: **https://belemdopara.org/datosyestadisticas/**

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

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

80. Para una tipologia de condutas que configuram violência de gênero facilitada por tecnologias e suas definições, 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). Disponível em: **https://digitallibrary.un.org/record/1641160?v=pdf**; y Luchadoras y SocialTic. Take back the tech! (2018). Disponível em: **https://www.takebackthetech.net/**

uma jovem relatou ter recebido mensagens intimidatórias com imagens de armas e ameaças contra sua família, além do vazamento de seu documento de identidade, aparentemente em retaliação por ter denunciado um caso de violência de gênero.

Esses casos, identificados durante o mesmo período de análise dos grupos e canais observados, ilustram alguns dos possíveis usos e finalidades da compra e venda de dados pessoais. A disponibilidade de informações pessoais amplia o alcance e a gravidade da violência facilitada pela tecnologia, transformando o acesso ilícito a dados em um meio que facilita a chantagem, o controle e o assédio. Nesse sentido, mais que incidentes isolados, esses episódios refletem os riscos estruturais de um ecossistema no qual a falta de segurança e de responsabilização na gestão de dados permite que a violência de gênero encontre novas ferramentas e formatos.

Da mesma forma, em alguns dos grupos peruanos analisados, foram observadas hierarquias funcionais e dinâmicas de interação marcadas por expressões abertamente homofóbicas e misóginas -como "Gato Gay"-, o que evidencia como os espaços digitais onde circulam dados pessoais também reproduzem e reforçam lógicas de dominação e exclusão baseadas em gênero e orientação sexual. Embora essas manifestações não derivem diretamente da compra e venda de informações, elas revelam o ambiente sociotécnico em que essa prática opera: um ecossistema permeado por discursos violentos e estruturas de poder baseadas em gênero que legitimam a exposição e o controle sobre identidades dissidentes.

As consequências desse tipo de violência são profundas, afetando tanto a esfera individual quanto a social. Afetam a saúde mental, a segurança pessoal e familiar, as oportunidades profissionais e a participação política e social das vítimas/sobreviventes[81]. Em muitos casos, levam à autoexclusão dos espaços digitais, restringindo o exercício dos seus direitos à liberdade de expressão e de associação[82]e geram efeitos negativos para o debate público, essencial nas sociedades democráticas.

O direito internacional e regional dos direitos humanos reconhece a VGFT como violência de gênero e, portanto, como uma violação dos direitos humanos. A Relatoria Especial da ONU sobre a Violência contra a Mulher[83], relatórios do Conselho de Direitos Humanos[84] e o Comitê da Convenção sobre a Eliminação de Todas as Formas de Discriminação contra a Mulher (CEDAW, sigla em inglês)[85] reconheceram que as tecnologias digitais podem ser usadas para reproduzir e amplificar a violência de gênero e alertaram para a necessidade de gerar políticas integrais que reconheçam a continuidade entre o online e o offline. No âmbito interamericano, a Convenção de Belém do Pará obriga os Estados a prevenir, punir e erradicar todas

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**

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. Disponível em: **https://digitallibrary.un.org/record/1641160?v=pdf**

84. Para mais informação, 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 mais informação, ver: **https://www.acnur.org/fileadmin/Documentos/BDL/2017/11405.pdf**

as formas de violência de gênero, inclusive aquelas facilitadas pela tecnologia[86].

Apesar dos progressos alcançados a nível internacional e regional, os quadros jurídicos nacionais sobre VGFT ainda não conseguiram garantir uma proteção efetiva para as mulheres e as pessoas LGBTQIA+. Em geral, as respostas dos Estados foram mais centradas na dimensão penal do que em medidas integrais de prevenção, reparação e acompanhamento às vítimas.

No Brasil, por exemplo, a situação normativa é bastante fragmentada. A pesar de contar com normas relevantes como a mencionada reforma do Código Penal de 2012 (também chamada Lei Carolina Dieckmann)[87], que tipifica delitos informáticos, e estabelece leis que criminalizam condutas como o *stalking*[88] e a violência política de gênero[89]; a Lei Fundacional contra a Violência de Gênero, n. 11.340/2006 (chamada de Lei Maria da Penha) não contempla expressamente a violência facilitada pelas tecnologias. Em consequência, o país precisa de um marco específico sobre VGFT que garanta às vítimas desse tipo de violência o acesso às medidas de proteção e reparação civil previstas na Lei Maria da Penha[90].

No Peru, a Lei 30364, de 2015[91] e o Decreto Legislativo 1410, de 2018[92], tipificaram modalidades de assédio, chantagem sexual e difusão de imagens íntimas, incluindo quando são cometidas mediante tecnologias. No entanto, persistem lacunas importantes: a definição de violência digital ainda é difundida, a norma não inclui de maneira explícita mulheres trans ou população LGBTIQA+, e sua abordagem criminosa faz com que muitas vítimas não sejam efetivamente protegidas e reparadas[93].

Por último, na Argentina, a já mencionada reforma penal de 2008[94] incorporou delitos on-line com o Convênio de Budapeste, mas sem perspectiva de gênero, o que deixou de fora condutas frequentes de VGFT como a difusão sem consentimento de imagens íntimas[95]. Apenas recentemente, em 2023, com a reforma da Lei 26.485, por meio da chamada Lei Olimpia Argentina[96], a violência digital foi reconhecida como uma categoria específica de violência de gênero e mecanismos

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

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

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

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

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

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

92. Disponível em: **https://busquedas.elperuano.pe/dispositivo/NL/1690482-3**

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

94. Disponível em: **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. Disponível em: **https://revistalatam.digital/article/i5-07/**

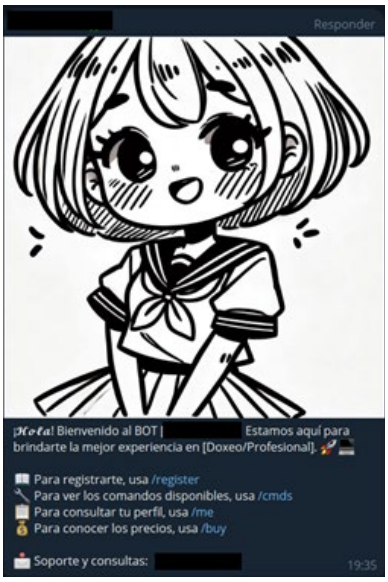
96. Disponível em: **https://www.boletinoficial.gob.ar/detalleAviso/primera/296572/20231023**

ágeis foram estabelecidos para lidar com ela, marcando um avanço significativo[97], embora sua eficácia dependa da implementação adequada e deva ser monitorada e avaliada nos próximos anos.

5.3 Riscos às infâncias on-line

Uma descoberta alarmante nos ambientes analisados é o uso recorrente de ilustrações em estilo anime, retratando garotas com aparência de uniforme escolar e características visuais típicas desse tipo de arte, como recurso gráfico para dar boas-vindas ou promover os serviços de grupos do Telegram, como pode ser visto nos exemplos abaixo (ver Imagem 10):

Imagem 10. Ilustrações em estilo anime usadas para dar as boas-vindas ou promover os serviços de grupos de venda de dados no Telegram.



Este não é um fenômeno isolado ou inocente: ele reproduz uma lógica mais ampla da publicidade na América Latina, em que a imagem de mulheres infantilizadas ou hipersexualizadas funciona como isca para capturar a atenção e garantir cliques e compras[98].

Essa descoberta ressalta que, além dos aspectos técnicos ou legais, esses ecossistemas exigem uma leitura crítico-cultural, na qual o design e a comunicação visual desempenham um papel central na normalização de práticas ilícitas.

Além disso, o uso desse tipo de imagem está ligado a um contexto mais amplo de violência sexual e objetificação de meninas e adolescentes na América Latina. A região apresenta algumas das taxas mais elevadas de abuso e exploração sexual infantil do mundo, o que se reflete em fenômenos como gravidez na adolescência e uniões precoces.

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. Disponível em: **https://revistalatam.digital/article/i5-07/**

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

No Brasil, por exemplo, o Anuário de Segurança Pública de 2025 relata que 76,8% de todos os casos de violência sexual registrados em 2024 foram "estupro de vulnerável" (vítimas menores de 14 anos), com predominância de incidentes intrafamiliares.[99] No Peru, de acordo com o Ministério da Mulher e das Populações Vulneráveis, de janeiro a setembro de 2024, os Centros de Emergência para Mulheres (CEM) atenderam mais de 46 mil casos de meninas, meninos e adolescentes vítimas de diferentes tipos de violência. Desse total, 16.447 (35,67%) correspondem à violência sexual, o que equivale a aproximadamente 54 pessoas menores de 18 anos sendo agredidas sexualmente por dia[100].

Embora sejam dados nacionais, eles ilustram um padrão regional de alta vitimização infantil, que também se reflete no Telegram, por meio do uso de uma estética visual hipersexualizada e infantilizada de mulheres, supostamente empregada como estratégia de recrutamento nos grupos.

Em consonância com o uso problemático de imagens de crianças, conforme discutido nas seções anteriores, a pesquisa identificou casos de venda de dados pessoais de meninas, meninos e adolescentes, bem como dados sobre parentesco e filiação. Considerando que essa população está em desenvolvimento físico, psicológico, emocional e social, a exposição de seus dados aumenta sua vulnerabilidade, tanto online quanto offline, a atos de violência como assédio e extorsão. Além disso, quando esses bancos de dados incluem dados familiares ou dados sobre cuidadores (como endereços, números de telefone ou laços familiares), o risco também se estende aos adultos responsáveis, que podem temer represálias ou tentativas de coerção dirigidas a eles ou a seus filhos.

Dada a especial vulnerabilidade das crianças e dos adolescentes, a Convenção das Nações Unidas sobre os Direitos da Criança estabelece a doutrina da proteção integral, que reconhece esses indivíduos como sujeitos de direitos e lhes garante medidas especiais de proteção. O Comentário Geral n. 25 do Comitê de Direitos da Criança[101], órgão de especialistas independentes da ONU, reconhece explicitamente que essa proteção se estende aos entornos digitais. Entre outras medidas, o Comentário recomenda aos Estados que revejam e atualizem a sua legislação para garantir que o ambiente digital seja compatível com os direitos das crianças; integrem a proteção online nas políticas de proteção infantil; exijam privacidade no design, proteção de dados robusta e cibersegurança em produtos e serviços utilizados por crianças e adolescentes; e garantam soluções rápidas e adequadas à idade. Da mesma forma, o texto legal detalha os princípios da minimização de dados, o consentimento informado (próprio ou de pessoas cuidadoras, de acordo com a idade e as capacidades) e os direitos de acesso, retificação e eliminação relacionados aos dados. Diante do exposto, é preocupante que esses princípios não sejam observados claramente nos contextos analisados na pesquisa.

99. Para mais informação, 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. Disponível em: **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. Disponível em: **https://www.ohchr.org/es/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation**

No que diz respeito às legislações nacionais do Brasil, Peru e Argentina, o panorama reflete avanços importantes (embora desiguais) na proteção de crianças e adolescentes em ambientes digitais, em consonância com a perspectiva do direito internacional. No Brasil, a Constituição Federal[102] consagra a prioridade absoluta na promoção e proteção dos direitos das crianças e dos jovens, operacionalizada pelo Estatuto da Criança e do Adolescente (Lei 8.069/1990)[103] por meio de políticas, justiça especializada e medidas de prevenção e resposta. Em relação aos dados pessoais, a LGPD (Lei 13.709/2018)[104] dedica um artigo ao tratamento de dados de crianças, impondo o princípio do interesse superior para qualquer atividade de tratamento dos seus dados.

No Peru, o Código de Niños e Adolescentes (Ley 27337)[105] também estabelece uma proteção abrangente e define as categorias etárias. A Lei de Delitos Informáticos (Lei 30096)[106] tipifica comportamentos de risco digitais, como o aliciamento online, e foi recentemente reforçada para promover o uso seguro e responsável das tecnologias por crianças e adolescentes. Por sua vez, a Lei de Proteção de Dados Pessoais (Lei 29733)[107] reconhece a necessidade de medidas especiais no tratamento de dados de pessoas com menos de 18 anos de idade, a serem desenvolvidas por meio de regulamentação e com uma abordagem baseada em direitos.

Na Argentina, a Lei de Proteção Integral dos Direitos de Meninas, Meninos e Adolescentes (Lei 26.061)[108], de 2005, estabelece o sistema de proteção para essas pessoas em nível federal. Na esfera criminal, o Código Penal (Lei 26.904)[109] criminaliza o assédio a pessoas com menos de 18 anos por meios eletrônicos e a Lei 27.590 (também conhecida como Lei Mica Ortega)[110] cria um programa nacional de prevenção e conscientização sobre *grooming* ou assédio virtual. Por sua parte, a Lei 25.326, de proteção de dados, não contém um capítulo específico para crianças e adolescentes, mas a AAIP emitiu guias e recomendações para sua proteção em ambientes digitais[111].

Os resultados sugerem que, mesmo com as leis existentes, persiste uma brecha crítica entre o reconhecimento formal e a proteção efetiva. A exploração de estética que hipersexualiza as meninas revela como se entrelaçam as violências de gênero e os exercícios contra a infância, gerando danos sobrepostos. Superar essa brecha requer instituições sólidas, medidas técnicas verificáveis e obrigações claras tanto para plataformas como para as autoridades, a fim de que os direitos não sejam meramente enunciados, mas efetivamente garantidos.

102. Disponível em: **https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm**

103. Disponível em: **https://www.planalto.gov.br/ccivil_03/leis/l8069.htm**

104. Disponível em: **https://www.planalto.gov.br/ccivil_03/leis/l8069.htm**

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

106. Disponível em: **https://lpderecho.pe/ley-delitos-informaticos-ley-30096/**

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

108. Disponível em: **https://www.argentina.gob.ar/normativa/nacional/110778/texto**

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

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

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

VOLTAR AO SUMÁRIO

6 RECOMENDAÇÕES

Esta seção reúne um conjunto de recomendações operacionais e específicas para enfrentar as vulnerabilidades e direitos identificados nos resultados desta pesquisa. Se organizam por projetos temáticos e, em cada um, se propõem ações gerais, com medidas específicas por país, quando corresponda.

A abordagem prioriza as medidas de atenção, proteção e reparação específicas às vítimas dos ataques e vulnerações de direitos identificados; a integração real das perspectivas de gênero e de infância e adolescência; o fortalecimento das instituições para a aplicação efetiva das leis existentes; e a governança e responsabilidade do setor público sobre dados. Dado o caráter transfronteiriço do mercado ilegal de dados, também são incorporadas medidas de cooperação regional, bem como obrigações reforçadas para plataformas. Todos amparados por padrões do direito internacional, com base na proporcionalidade, no devido processo e nos direitos humanos.

6.1 Atenção e reparação a vítimas com dados em circulação no mercado ilegal

Os casos identificados pela pesquisa, assim como os não mapeados que circulam nos mercados já estabelecidos, mostram que, além de ajustes arquitetônicos legais e institucionais, é imprescindível situar as pessoas afetadas pela compra e venda de seus dados no centro. Uma resposta eficaz requer serviços acessíveis, gratuitos e sensatos, com rotas claras de pesquisa e atuação coordenada entre atores como autoridades, plataformas, operadoras de pagamento e telecomunicações. Em outras palavras, e de acordo com o Protocolo La Esperanza[112], a resposta a vítimas deve ser integral, sensível ao trauma e centrada nos direitos das pessoas afetadas.

Por isso, se recomenda:

- Realizar operações de pesquisa e mapeamento integral do mercado ilegal de dados no Telegram para dimensionar sua escala, estrutura e danos; conformar equipes conjuntas entre autoridades de proteção de dados, promotores, equipes de resposta a incidentes e a emergências em Segurança Cibernética CERT (*Computer Emergency Response Team*, em inglês) CSIRT (*Computer Security Incident Response Team*, em inglês) defensorias, com o apoio da sociedade civil e da academia.

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

• Garantir patrocínio jurídico gratuito quando for o caso e representação especializada para solicitar administrativa ou judicialmente medidas cautelares, incluindo: remoção de conteúdo, ordens de não contato, proibição de divulgação, preservação de provas e, quando corresponda, alteração célere de documentos e credenciais comprometidos.

• Fornecer suporte por meio de equipes técnicas de resposta que dimensionem a extensão do dano, identificam os sistemas e ambientes afetados, configurando alertas para novas ocorrências e restaurando o acesso privado e seguro.

• Empregar equipes psicossociais com foco em gênero e infância para atenção integral e sensível ao trauma, com protocolos claros de confidencialidade, consentimento informado e encaminhamento seguro. Garantir a acessibilidade para pessoas com deficiência e a cobertura em línguas indígenas, quando relevante.

• Operacionalizar o direito ao apagamento e à desindexação, quando apropriado, garantindo a remoção do conteúdo dentro de prazos urgentes.

• Notificar proativamente os indivíduos potencialmente afetados quando uma violação de dados pessoais for verificada, informando-os sobre os riscos, as medidas tomadas e as etapas de proteção recomendadas, e oferecer assistência imediata. Priorizar crianças e adolescentes, mulheres e pessoas LGBTQIA+, bem como pessoas em situação de vulnerabilidade por outros motivos, como razões étnico-raciais ou territoriais.

• Padronizar os protocolos de preservação de provas e de cadeia de custódia para evitar que as vítimas tenham que expor novamente informações sensíveis. Disponibilizar canais seguros para o envio de provas, minimizar a coleta de dados adicionais e limitar a retenção ao tempo estritamente necessário.

• Estabelecer mecanismos acessíveis para reclamações e recursos para os casos em que a resposta do Estado ou das plataformas for tardia ou insuficiente, com revisão independente, prazos definidos e a obrigação de justificar cada decisão.

6.2 Violência de gênero facilitada por tecnologias

A venda e o uso de dados pessoais intensificam padrões de controle, extorsão e silenciamento que já afetam desproporcionalmente mulheres e pessoas LGBTQIA+. Para a sua proteção, é necessária a integração efetiva da perspectiva de gênero nas políticas de proteção de dados e segurança cibernética, bem como medidas integrais, ordens de proteção digital e serviços de apoio.

• Reconhecer o VGFT como uma violação dos direitos humanos e violência de gênero, garantindo que as leis estejam integradas com medidas de proteção digital para as vítimas de ataques, como a remoção rápida de conteúdo prejudicial, bloqueio de contato, proibição de disseminação e a preservação de provas. Isso é especialmente importante no caso do Brasil, que não reconhece explicitamente a violência de gênero facilitada pela tecnologia como uma forma de violência de gênero em seu sistema jurídico.

• Estabelecer protocolos intersetoriais entre órgãos públicos, como as autoridades de proteção de dados e os CERT/CSIRTs nacionais, a polícia, o Ministério Público, os funcionários do judiciário e os órgãos de atenção a vítimas de violência de gênero para casos que envolvam a utilização de dados adquiridos e/ou vazados, de forma que exista um percurso único, integrado e protetivo de apoio, em conformidade com as normas do Protocolo La Esperanza.[113]

• Proporcionar formação obrigatória e contínua sobre questões de gênero e violência digital para as autoridades de proteção de dados e cibersegurança, ministérios públicos, poder judicial e defensorias.

• Implementar o monitoramento e publicar dados desagregados por gênero e identidade nos registros de incidentes, com relatórios públicos.

6.3 Proteção das infâncias

Crianças e adolescentes são pessoas em fase de desenvolvimento físico, mental, emocional e social, que têm direito à proteção integral e específica. A venda de seus dados e o uso de estética hipersexualizada em grupos e canais do Telegram reforçam práticas ilícitas e aumentam os riscos à segurança deles e de suas famílias. São necessárias normas de projeto, restrições comerciais e serviços de proteção adequados à idade.

Por isso, se recomenda:

• Estabelecer normativas aplicáveis a serviços e produtos digitais direcionados ou acessíveis a crianças e adolescentes que garantam, por padrão, máxima privacidade e segurança, minimizando rigorosamente os dados processados e medidas reforçadas de cibersegurança.

• Exigir avaliações de impacto específicas e sobre os direitos das crianças obrigatórias para sistemas públicos e privados que processam dados de crianças e adolescentes, bem como para serviços digitais massivos utilizados por crianças e adolescentes. Incluir na metodologia dessas avaliações de impacto etapas de consulta significativa com crianças, adolescentes e especialistas.

• Garantir que os serviços de tecnologia voltados para a educação e aplicados a bancos de dados de escolas e departamentos de educação priorizem a segurança e a privacidade desde a sua concepção, proibindo a coleta de dados desnecessários e o rastreamento por terceiros; limitando o acesso, auditando fornecedores e contratos, definindo cronogramas de retenção e exclusão de dados e oferecendo alternativas não digitais para evitar a exclusão. Além disso, capacitar professores e equipes escolares em proteção, resposta a incidentes e apoio psicossocial.

• Implementar linhas de apoio especializadas e equipes psicossociais com protocolos de mitigação de danos digitais para crianças e adolescentes, ou fornecer treinamento sobre o assunto para as equipes existentes em questões digitais.

113. Ibid.

6.4 Cumprimento legal e autonomia institucional

Brasil, Peru e Argentina possuem leis de proteção de dados, embora com diferentes graus de desenvolvimento e, em alguns casos, sem disposições específicas para o setor público. Também possuem estratégias de segurança cibernética e leis penais relacionadas a crimes informáticos. No entanto, as evidências mostram que a existência dessas leis não é suficiente para garantir ampla proteção dos cidadãos contra os mercados de compra e venda de dados no Telegram. A discussão, portanto, deve ir além do âmbito normativo e se concentrar na aplicação efetiva das leis, bem como na necessidade de dotar as autoridades de poderes e capacidades suficientes para supervisionar e sancionar, inclusive o próprio Estado, quando este incorrer em violações de direitos.

Portanto, se recomenda:

- Garantir a autonomia institucional das autoridades de proteção de dados e segurança cibernética em relação aos governos. Essa autonomia deve incluir mecanismos de supervisão civil independente, responsabilização e proteção contra interferência política. Isso é especialmente relevante nos casos do Peru e da Argentina, onde as autoridades estão integradas sob a arquitetura institucional dos ministérios de Estado e de inteligência, respectivamente.

- Garantir orçamentos plurianuais adequados para as autoridades de proteção de dados e para os CERT/CSIRTs nacionais, com regras claras que limitem a interferência política externa. Garantir que essas instituições tenham escalas salariais competitivas e uma carreira técnica que atraia e retenha pessoal importante, para que elas tenham a capacidade efetiva de supervisionar e responder a incidentes. Isso é fundamental no caso do Brasil, cuja autoridade de proteção de dados é independente, mas tem capacidade limitada de atuação devido a restrições orçamentárias e de pessoal.

- Conceder institucionalmente poderes de sanção eficazes contra entidades privadas e públicas. Ordenar a publicação de sanções e de medidas adotadas a fim de gerar efeitos de dissuasão e fortalecer a transparência.

- Capacitar tribunais e promotores em temas como crimes cibernéticos, proteção de dados e violência digital, com protocolos de cadeia de custódia e guias para provas eletrônicas.

- Estabelecer canais seguros para denunciantes (*whistleblowers*) que garantam confidencialidade, proteção contra represálias e mecanismos de monitoramento público das medidas implementadas.

- Publicar relatórios periódicos e painéis de controle públicos sobre incidentes de segurança e vazamentos que afetam os dados dos cidadãos, em formatos abertos e acessíveis, com proteção de identidade por meio de medidas de anonimização e pseudonimização. Desagregar la informação por indicadores como gênero e faixas etárias para orientar políticas públicas e focalizar medidas de prevenção e reparação.

6.5 Governança de dados públicos e responsabilidade dos Estados

As evidências sugerem que uma parcela significativa dos dados comercializados pode ter origem em bancos de dados estaduais ou em serviços públicos a eles vinculados. A digitalização acelerada dos Estados, sem controles equivalentes de segurança, auditoria e transparência, criou superfícies de ataque e abusos internos que exigem regras e capacidades reforçadas, distintas daquelas do setor privado.

Por isso, se recomenda:

- Estabelecer um regime jurídico reforçado para o setor público: revisão ou reforma de leis ou regulamentos específicos que estabeleçam responsabilidades diferenciadas para os Estados no tratamento de dados pessoais. Além de maior transparência, essas regulamentações devem estabelecer medidas para restringir o uso secundário de dados, reforçar princípios como a minimização, garantir o exercício de direitos e proibir consultas em massa sem justificativa caso a caso.

- Minimizar os dados coletados e armazenados por instituições públicas, limitando-os aos princípios da necessidade e da adequação.

- Políticas de cibersegurança em instituições públicas que gerenciam bancos de dados, incluindo gerenciamento de acesso adequado, aplicando o princípio do mínimo privilégio, de forma que cada funcionário acesse apenas as informações estritamente necessárias para o desempenho de suas funções; bem como a revogação imediata das credenciais quando mudam de cargo ou deixam a instituição. Além disso, implementar mecanismos de monitoramento usando alertas em tempo real para detectar consultas automatizadas e em grande escala incomuns nos bancos de dados.

- Os dados pessoais devem ser criptografados tanto em trânsito quanto em repouso, reduzindo assim a probabilidade de exposição. Os ambientes de teste também devem ser separados dos ambientes de produção, e técnicas de mascaramento ou anonimização de dados devem ser aplicadas às consultas que não exigem a exibição de informações completas.

- Realizar testes de penetração regulares em seus sistemas para identificar vulnerabilidades antes que sejam exploradas por terceiros. Esses testes devem incluir cenários de ataque externos e simulações de ameaças internas, garantindo que não sejam coletados ou processados mais dados pessoais do que o estritamente necessário para sua execução e análise, de acordo com o princípio da minimização.

- Notificação obrigatória de violação de dados públicos, com prazos curtos, registros públicos de incidentes, análise da causa raiz e plano de remediação verificável.

- Auditorias externas periódicas de bases de dados públicas, especialmente aquelas que contêm registros críticos como identidade, licenças, educação, saúde, crédito e programas sociais, e publicação de seus resultados. Essas au-

ditorias devem incluir, além de uma avaliação técnica de segurança, avaliações de impacto sobre os direitos humanos e transparência ativa em relação às suas conclusões, em conformidade com as diretrizes do Protocolo La Esperanza.[114].

• Contratação e aquisição seguras: adicionar cláusulas de cibersegurança e privacidade desde a concepção aos contratos públicos relacionados a sistemas de armazenamento de dados e priorizar contratos de software de código aberto, incluindo auditorias de código público, transparência de dependências e interoperabilidade baseada em padrões abertos.

6.6 Governança de plataformas digitais

Os resultados indicam que no Telegram, sem prejuízo da verificação de práticas semelhantes em outras plataformas, a compra e venda de dados pessoais é realizada por meio de *bots*, *gateways* de pagamento e opacidade operativa. Nesse contexto, é crucial considerar a responsabilidade das plataformas sob a perspectiva dos padrões de direitos humanos.

Isso implica avançar em direção a uma governança baseada nos princípios da legalidade, necessidade e proporcionalidade, com garantias de devido processo e mecanismos de transparência eficazes por meio de relatórios e auditorias acessíveis. Exige-se também uma maior diligência prévia em relação a *bots* e sistemas automatizados, verificação de desenvolvedores e fluxos de monetização, incorporação de limites e salvaguardas técnicas proporcionais ao risco e a existência de mecanismos eficazes de reparação para as vítimas, preservando simultaneamente a privacidade e a liberdade de expressão.

Por isso, se recomenda:

• Habilitar sistemas acessíveis para que as pessoas usuárias possam denunciar *bots* suspeitos, além de implementar mecanismos de detecção para identificar *bots* que acessam ou processam dados pessoais, com o acompanhamento de organizações de direitos humanos.

• Publicar relatórios periódicos sobre a remoção e o cumprimento de ordens legais e judiciais, com dados agregados e desagregados por tipo de abuso, gênero e faixa etária, quando apropriado.

• Estabelecer um canal de resposta rápida para ordens judiciais de remoção de conteúdo, credenciando organizações da sociedade civil e acadêmicas como *trusted flaggers* (sinalizadoras confiáveis), comprometendo-se com prazos urgentes para mitigar riscos elevados e documentando os critérios de priorização e os resultados de cada intervenção.

• Reforçar a coordenação entre as agências policiais, as plataformas de pagamento e os serviços financeiros para identificar fluxos ligados à comercialização ilícita de dados pessoais, com base em análises de risco e investigações ou denúncias formais, evitando o rastreamento indiscriminado de transações.

114. Ibid.

• Exigir transparência operacional para *bots* e automações, publicando termos de uso específicos, regras para coleta e processamento de dados, fontes de treinamento ao usar IA e expondo métricas de segurança e conformidade, com auditorias independentes e termos acessíveis ao público.

• Garantir mecanismos eficazes de reparação para as vítimas de violações em seus ambientes, oferecendo canais claros de denúncia dentro da plataforma, priorizando a remoção de conteúdo que revele dados sensíveis e permitindo a desindexação e a prevenção de sua republicação, com salvaguardas para a liberdade de expressão e o devido processo.

• Aplicar o princípio da proporcionalidade em todas as medidas, minimizando os impactos sobre as pessoas usuárias que fazem uso lícito dos serviços, preservando a privacidade por meio da criptografia de ponta a ponta e combinando ferramentas técnicas e de governança necessárias e adequadas à finalidade pretendida, avaliando regularmente sua eficácia e possíveis efeitos adversos.

• Designar um responsável legal com domicílio e poderes suficientes em cada país onde as plataformas operam, registra-lo junto às autoridades e reguladores correspondentes e manter um ponto de contato para autoridades e pessoas usuárias. Garantir que tal responsável possa receber notificações e ordens judiciais ou administrativas e cumprir os prazos e requisitos locais, assegurando simultaneamente a observância das normas internacionais e regionais de direitos humanos.

6.7 Cooperação regional e transfronteiriça

O mercado ilegal de dados e a dinâmica da violência identificados nesta pesquisa operam, em muitos casos, em escala transfronteiriça. A cooperação regional, nesse sentido, é chave. Para isso, se recomenda:

• Formar equipes regionais conjuntas de pesquisa para casos de venda de dados, *doxxing* e extorsão, estabelecendo critérios de ativação, objetivos, prazos e métricas de sucesso.

• Publicar relatórios regionais de transparência com estatísticas comparáveis sobre incidentes, tempos de resposta, sanções e reparações para as vítimas, avaliando os impactos, as salvaguardas para a liberdade de expressão e privacidade, e documentando as metodologias.

• Fortalecer as redes e os organismos de colaboração regional em matéria de proteção de dados e cibersegurança, como a Rede Ibero-Americana de Proteção de Dados e a Organização dos Estados Americanos, enquanto plataformas operativas para a produção de provas e a coordenação de políticas em casos de violações de direitos, como a compra e venda de dados pessoais, bem como vazamento de bases de dados públicas, criando grupos de trabalho permanentes com objetivos e cronogramas, e alocando um orçamento para apoio técnico forense.

• Estabelecer protocolos para a preservação de provas digitais e a circulação transfronteiriça dessas provas, com base em normas de direitos humanos e em parâmetros de legalidade, necessidade e proporcionalidade.

• Definir salvaguardas para investigações em contextos transfronteiriços.

• Garantir a proteção e a reparação transfronteiriça para vítimas, quando apropriado, homologando ordens de proteção digital entre países e ativando redes de apoio institucional para as vítimas quando a pessoa afetada se encontrar fora do seu país.

• Garantir que toda a cooperação empreendida incorpore avaliações de impacto sobre os direitos humanos, bem como mecanismos de recurso e responsabilização, publicando resumos das operações, resultados e lições aprendidas, sem expor as vítimas ou comprometer as investigações em curso.

WWW.DERECHOSDIGITALES.ORG