Governo

Bots no Telegram expõem dados de brasileiros em segundos por menos de R$ 6

ONG Derechos Digitales mapeou mercado ilegal que comercializa CPF, renda, empregos, vacinação e benefícios sociais de qualquer pessoa.

Luís Osvaldo Grossmann • 13 de março de 2026 3 minutos de leitura

O Brasil aparece como um dos principais focos de um mercado ilegal de dados pessoais operado dentro do Telegram, segundo pesquisa "Identidades à venda: o mercado ilegal de compra e venda de dados pessoais latino-americanos no Telegram", da Derechos Digitales. O estudo identificou dez grupos ativos no país dedicados à venda de informações confidenciais de cidadãos por meio de bots automatizados, que permitem consultar em segundos dados associados a CPF, nome ou telefone mediante pagamento via Pix.

No total, a investigação localizou 27 grupos e canais ativos no Brasil, Peru e Argentina que funcionam como verdadeiras "lojas de dados" dentro da plataforma. Nesses espaços, usuários podem realizar consultas gratuitas limitadas, geralmente revelando apenas nome e CPF, e, mediante pagamento, acessar informações muito mais detalhadas, como endereço, histórico de emprego, renda estimada, registros de benefícios sociais e até dados de vacinação.

No caso brasileiro, os pesquisadores observaram um alto grau de automação. Todos os grupos analisados possuem ao menos um bot configurado como administrador, capaz de responder automaticamente a comandos e entregar os resultados das consultas sem intervenção humana. Essa estrutura permite que os grupos operem 24 horas por dia como serviços de busca de dados pessoais. Paralelamente, administradores humanos atuam sob pseudônimos como “dono”, “admin” ou “suporte”, organizando a gestão do grupo de forma descentralizada e anônima.

O modelo de negócio predominante identificado é o freemium: consultas básicas são gratuitas, mas o acesso completo exige pagamento. Os preços variam de cerca de US$ 1 por uma semana de acesso até quase US$ 80 por dois anos. Promoções temporárias e anúncios com urgência, como ofertas válidas “somente hoje”, reproduzem estratégias típicas do marketing digital em um ambiente ilegal.

Os pagamentos são feitos via Pix. Embora a ferramenta tenha sido criada para reduzir custos e aumentar a rastreabilidade das transações, o relatório aponta que ela também vem sendo explorada em atividades ilícitas. Nos grupos analisados, os pagamentos geralmente são processados por códigos gerados em plataformas intermediárias de cobrança digital.

O principal mecanismo de consulta identificado nos grupos brasileiros é o comando “/cpf”. Ao inserir o número do documento, o bot gera um arquivo estruturado com informações detalhadas da pessoa pesquisada. O relatório descreve que essas fichas incluem nome completo, RG, data de nascimento, sexo, município de origem e histórico de endereços, além de dados econômicos como estimativa de renda e classificação de poder aquisitivo.

Os registros também podem trazer pontuações de risco de crédito e perfis de consumo semelhantes aos utilizados por birôs de crédito, como Serasa e SPC Brasil. Em alguns casos, os bots retornam informações de emprego que reproduzem campos típicos de registros oficiais, incluindo profissão, código da ocupação, empresa empregadora, salário, escolaridade e datas de admissão.

Além disso, os arquivos analisados incluem dados extremamente sensíveis, como o número do Programa de Integração Social (PIS), histórico de benefícios sociais, entre eles o Bolsa Família e o Auxílio Emergencial, e informações de contribuições ao Instituto Nacional do Seguro Social. Em

alguns casos, também foram identificados registros detalhados de vacinação vinculados ao sistema público de saúde.

Segundo os pesquisadores, a estrutura dos dados e a presença de elementos técnicos típicos de bancos de dados estruturados — como campos padronizados e valores nulos — indicam que as informações podem ter sido extraídas diretamente de bases institucionais ou de grandes bancos de dados integrados.

A exposição não se limita à pessoa consultada. Em diversos registros, aparecem dados de familiares, como irmãos e sobrinhos, além de informações de vizinhos. Isso permite mapear redes de relacionamento e amplia os riscos de fraude direcionada, extorsão ou vigilância.

A pesquisa alerta que a circulação massiva dessas informações pode facilitar crimes como fraudes financeiras, roubo de identidade, extorsão, assédio digital e violência de gênero. Mulheres, crianças e pessoas LGBTIQA+ estão entre os grupos mais vulneráveis a esse tipo de exposição.

“O Estado coleta dados dos cidadãos para prestar serviços e, muitas vezes, reúne informações sensíveis que, se não forem tratadas com o devido cuidado, podem colocar as pessoas em risco”, afirmou Rafael Bonifaz, líder do Programa Latino-Americano para Resiliência e Defesa Digital da Derechos Digitales. “Nesta investigação, mostramos os desafios que ainda existem na proteção dessas informações e o quão acessíveis elas podem se tornar em plataformas como o Telegram.”

O relatório conclui que a América Latina enfrenta dificuldades para transformar suas leis de proteção de dados em garantias efetivas. Entre os problemas apontados estão lacunas regulatórias no tratamento de informações pelo setor público, limitações na autonomia das autoridades de proteção de dados e fragilidades nas práticas institucionais de segurança da informação.

Entre as recomendações apresentadas estão o fortalecimento da governança de dados públicos, maior autonomia e recursos para autoridades de proteção de dados, incorporação de perspectivas de gênero e infância nas políticas de segurança da informação e maior responsabilização das plataformas digitais pela circulação ilícita de dados.

#Crimes cibernéticos #Crimes na Web #Dados #Manchete

Siga-nos Google News