



Clique e Assine por somente R\$ 2,50/semana

Economia

## Vazamento de dados: Claro, Oi, Tim e Vivo podem ser multadas em R\$ 60 mi

Operadoras são notificadas sobre o vazamento de 103 milhões de contas de celular e têm 15 dias para responder; irregularidades podem culminar em sanções

Por **Diego Gimenes** Atualizado em 16 fev 2021, 18h10 - Publicado em 16 fev 2021, 17h01



Microsoft/Divulgação

Uma semana após o **vazamento** de 102.828.814 de contas de celular, pouco se sabe a respeito da origem e ainda menos sobre quais seriam as punições aos criminosos. A exposição desses dados foi revelada pela empresa de cibersegurança PSafe na última quarta-feira, 10, e desde então as autoridades brasileiras buscam respostas para a ofensiva dos hackers. O Departamento de Proteção e Defesa do Consumidor, do **Ministério da Justiça**, notificou as operadoras **Claro, Oi, Tim e Vivo** e cobrou explicações sobre o assunto. As companhias têm 15 dias para



Consumidor e mais de 50 milhões de reais pela Lei Geral de Proteção de Dados (LGPD), de acordo com a pasta.

Procuradas pela reportagem, as operadoras negaram envolvimento no vazamento de informações e afirmaram que vão colaborar com as investigações do poder público.

Dentre as vítimas do ataque está o presidente Jair Bolsonaro, que teve informações como valor da conta, minutos gastos por dia, número do celular, filiação, data de nascimento e CPF vazadas na chamada *deepweeb* — uma camada mais profunda da internet, em que mensagens são trocadas de forma mais anônima. [Segundo a Psafe](#), o hacker vive fora do Brasil e está vendendo cada registro por 1 dólar, via bitcoin. A localização exata e a identidade não foram reveladas “pelo ambiente ser de difícil rastreamento”.

O ataque ocorreu um mês após o maior vazamento de dados da história do Brasil — quando 223 milhões de CPFs, 40 milhões de CNPJs e 104 milhões de registros de veículos foram divulgados. Segundo especialistas consultados por VEJA, a onda de ataques não é recente e os vazamentos sempre ocorreram, seja em maior ou menor grau, mas que a não obrigatoriedade de as empresas notificarem a Autoridade Nacional de Proteção de Dados (ANPD) tendia a acobertar vazamentos.

#### RELACIONADAS



Tecnologia

**Maior vazamento de dados pessoais do país expõe riscos da era digital**



Tecnologia

**Novo vazamento expõe mais de 100 milhões de contas de celular do Brasil**



Brasil

**OAB pede investigação do vazamento de dados de 220 milhões de pessoas**

“A LGPD exige que as companhias notifiquem ataques e vazamentos de dados. Outros países têm histórico de décadas em proteção de dados, mas o Brasil foi um dos últimos a aplicar uma legislação específica”, afirma Gisele Truzzi, advogada especialista em direito digital e proprietária do escritório Truzzi Advogados. A LGPD está em vigor no Brasil desde setembro de 2020. “Tendo conhecimento disso, os criminosos sabem que os bancos de dados brasileiros são mais vulneráveis, com legislação recente e cibersegurança falha.”

Ainda que a regulação seja nova e os cidadãos não tenham total controle do compartilhamento de seus dados pessoais na internet, é possível fugir dos crimes virtuais e evitar que informações sensíveis caiam na mão de criminosos. Os especialistas recomendam desconfiar de links que ofereçam promoções, trabalhos e oportunidades imperdíveis, não preencher formulários antes de certificar que o site é verdadeiro, ativar a autenticação de dois fatores nas redes sociais e evitar a divulgação de informações sensíveis em ambientes públicos, [como a chave Pix](#). “O brasileiro tem a cultura de colocar cadeado na porta só depois que o ladrão entra. Muitas pessoas e empresas subestimam o alto potencial da internet para a comercialização e uso indevido de dados e informações pessoais”, alerta Truzzi.

CONTINUA APÓS PUBLICIDADE