TozziniFreire.
ADVOGADOS

Boletim Cybernews.

2ª Edição | 2025

Este boletim é um informativo
da área de **Cybersecurity & Data Privacy**
de TozziniFreire Advogados.

SUMÁRIO

Clique na notícia e navegue pelo documento

INTRODUÇÃO

Nesta edição do Boletim Cybernews, destacamos as principais notícias sobre proteção de dados nos meses de fevereiro e março de 2025.

A 2ª Turma do STJ manteve decisão que rejeitou pedido de indenização por danos morais de R$ 10 milhões feito por uma empresária presa que alegou ter sofrido exposição midiática excessiva devido ao vazamento de informações sigilosas por agentes públicos.

Além disso, a 3ª Turma decidiu que basta o endereço de IP para que os provedores de conexão forneçam os dados cadastrais dos usuários, mesmo sem prévio fornecimento de porta lógica (que permite a individualização e identificação dos usuários em casos de endereços de IP compartilhados) pelos provedores de aplicação de internet.

Por fim, a 3ª Turma também fixou o entendimento de que o banco não pode ser responsabilizado pelo "golpe do motoboy" – no qual terceiros entram em contato com a vítima, informando que seu cartão haveria sido clonado, e solicitando que o consumidor digite a senha para desbloqueio – caso não seja provado o vazamento de dados.

LEGISLAÇÃO BRASILEIRA

ANPD, LGPD e descontos em medicamentos: desafios para o setor farmacêutico

Em março, as sócias da área de proteção de dados, Luiza Sato e Carla Battilana, realizaram uma visita à Autoridade Nacional de Proteção de Dados (ANPD) para discutir temas atuais e de interesse do mercado relacionados à proteção de dados. Durante a reunião, a ANPD, por meio de seu diretor, destacou a importância de diversos aspectos que são fundamentais para a conformidade das empresas com a Lei Geral de Proteção de Dados (LGPD).

Princípios

Com relação aos princípios, um dos principais pontos abordados foi a importância da **transparência**. Em termos práticos, as empresas devem ser sempre claras e abertas sobre como tratam os dados pessoais, garantindo que os titulares dos dados estejam sempre informados sobre a forma pela qual suas informações são tratadas.

No que diz respeito à **finalidade**, diante de um tratamento posterior dos dados pessoais, é importante que esse seja compatível com os propósitos originais informados ao titular, ainda que não seja idêntico.

Práticas de conformidade

Além disso, foi destacada a importância de as empresas estruturarem um **programa de conformidade** com a LGPD, de implementarem e seguirem uma **política de retenção e eliminação de dados**, além da elaborarem e manterem, quando for o caso, **Relatórios de Impacto à Proteção de Dados (RIPD)** atualizados, documentando as atividades de tratamento de dados que envolvam riscos e que estejam prontos para serem fornecidos quando solicitados pela ANPD.

Essas medidas são consideradas essenciais pela ANPD para que as empresas demonstrem sua conformidade com a LGPD e, assim, possam evitar sanções ou, ao menos, servir como atenuantes durante um processo de fiscalização.

Tempestividade

Por fim, a ANPD ressaltou a **importância de que suas solicitações de informações sejam respondidas tempestivamente**, nos termos das Resoluções CD/ANPD nº 1/2021 e nº 4/2023. Isso porque eventual ausência de

resposta pode ser considerada violação a tais normas e, consequentemente, ser levada em consideração na definição de eventual sanção a ser aplicada.

Nota Técnica ANPD nº 6/2025

Como se imagina, a não observância desses e outros aspectos podem resultar em sanções pela ANPD. Recentemente, isso pode ser observado no caso envolvendo a rede de farmácias RaiaDrogasil, o programa de fidelidade Stix e a Federação Brasileira das Redes Associativistas e Independentes de Farmácias (Febrafar).

Essas entidades foram alvo da Nota Técnica emitida pela coordenação-geral de Fiscalização da ANPD em fevereiro de 2025, marcando, enfim, a **conclusão de um processo de fiscalização** iniciado em maio de 2023, focado no **tratamento de dados pessoais pelas redes de drogarias e operadores de programas de fidelização e benefícios**.

Entrando em mais detalhes sobre o caso, a investigação foi instaurada com o objetivo de averiguar a conformidade das práticas adotadas por essas entidades com a LGPD. A ANPD voltou sua atenção para essas práticas em razão de preocupações relacionadas à forma pela qual os **dados pessoais sensíveis**, especialmente aqueles relacionados à saúde, estavam sendo tratados no âmbito de **programas de fidelidade**, os quais muitas vezes envolvem a personalização de ofertas e benefícios baseados no **perfil de consumo dos clientes das drogarias**.

Entre os pontos de atenção levantados em sua Nota Técnica, a ANPD destacou três principais preocupações:

I. **Monetização de dados de saúde:** dados relativos à saúde estavam sendo monetizados para fins de publicidade direcionada sem a devida transparência ou base legal adequada, o que poderia constituir um desvio das finalidades originalmente informadas aos titulares dos dados.

II. **Coleta de biometria:** a coleta de biometria – que também se enquadra como um tipo de dado pessoal sensível – ocorria sem considerar alternativas menos invasivas que poderiam atender aos mesmos propósitos de autenticação nos programas de fidelização, levantando questões sobre a necessidade e proporcionalidade do tratamento desse dado.

III. **Clareza sobre armazenamento e eliminação:** a falta de informações claras sobre os prazos de armazenamento e os procedimentos de eliminação de dados pessoais também foi identificada como uma falha, sugerindo uma possível violação ao princípio da necessidade, conforme exigido pela LGPD.

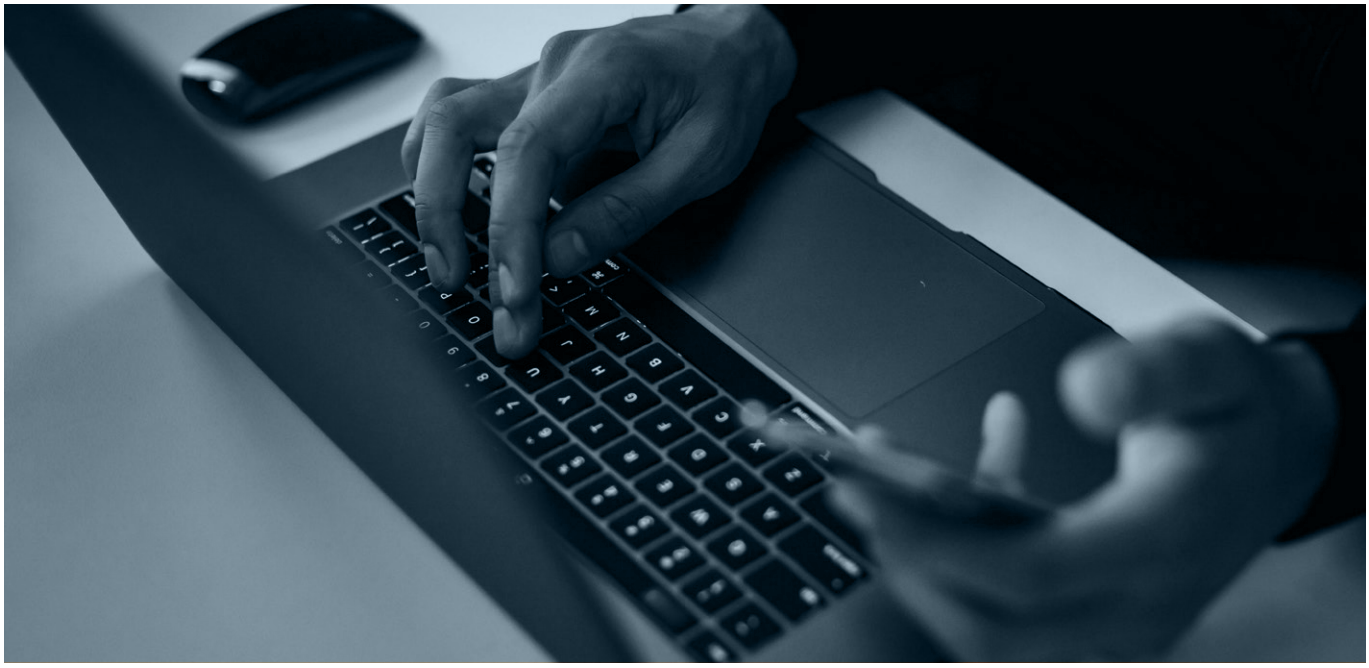
Em resposta às irregularidades observadas, a ANPD impôs uma série de medidas preventivas específicas às entidades, bem como instaurou um Processo Administrativo Sancionador contra a RaiaDrogasil para averiguar potenciais irregularidades envolvendo

o tratamento de dados pessoais para fins de formação de perfis comportamentais sem o devido amparo em base legal.

Com relação às medidas preventivas, a autoridade determinou que, entre outras, caberá à RaiaDrogasil implementar **métodos alternativos de verificação de identidade** para os clientes (que não exijam dados biométricos), adotar **medidas de transparência** com os titulares (e com a própria ANPD) sobre o armazenamento de dados pessoais e, ainda, esclarecer para a ANPD informações sobre **como os dados pessoais sensíveis são usados para criar perfis comportamentais**. Já para a Febrafar, as medidas preventivas incluem a necessidade de implementar **melhorias na comunicação** de políticas de privacidade no site da federação, para **facilitar o exercício dos direitos dos titulares**.

Por fim, a Nota Técnica reforça a relevância de **fortalecer as medidas de transparência com os titulares**, o que inclui fornecer informações claras e acessíveis sobre as finalidades do tratamento de seus dados pessoais, o período de armazenamento e os procedimentos disponíveis para o exercício dos seus direitos.

Independentemente de os argumentos apresentados pelos agentes fiscalizados terem sido suficientes ou de alguns pontos levantados pela ANPD serem passíveis de questionamento, o principal recado que fica, inclusive em consonância com as informações obtidas durante a visita a ANPD em março, é a necessidade de implementar um programa de conformidade robusto e conduzir a devida avaliação de impacto para atividades de tratamento de dados pessoais, especialmente quando envolvem dados sensíveis. Essas medidas não apenas demonstram o compromisso das empresas com a proteção de dados, mas também funcionam como mecanismos de defesa diante de eventuais questionamentos e fiscalização.



NOTÍCIAS GERAIS

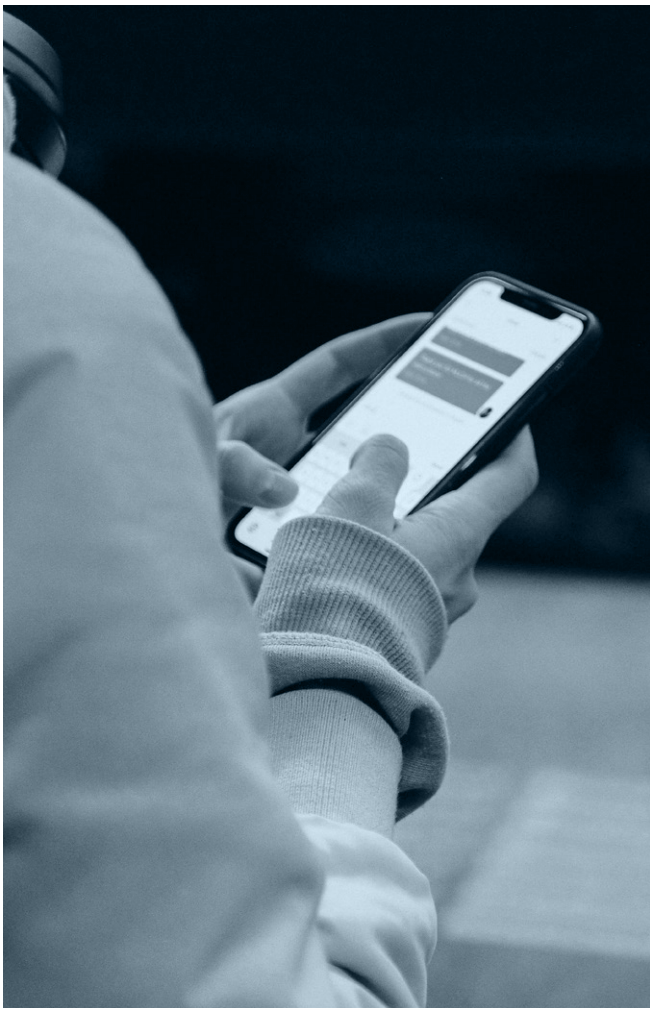
União não deve indenizar empresária por vazamento de informações por agentes públicos

A 2ª Turma do Superior Tribunal de Justiça (STJ) não reapreciou um pedido de indenização por danos morais contra a União feito por uma empresária envolvida na Operação Satiagraha, que alegou sofrer exposição midiática excessiva devido ao vazamento de informações sigilosas por agentes públicos.

A empresária pedia R$ 10 milhões em indenização, mas o pedido foi julgado improcedente em primeira instância, pela ausência de nexo entre os fatos narrados pela imprensa e os danos alegados. O Tribunal Regional Federal (TRF) da 2ª Região confirmou essa decisão, levando a empresária a recorrer ao STJ.

Em recurso especial, a empresária argumentou que o TRF não considerou provas sobre a conduta ilícita de agentes públicos e fatos novos, como a condenação do delegado da operação por violação de sigilo profissional. No entanto, a 2ª Turma do STJ manteve a decisão anterior, negando a indenização.

Em conclusão, a decisão do STJ ressalta a importância da necessidade de um vínculo claro entre os atos de agentes públicos e os danos alegados para a concessão de indenização por danos morais devido ao vazamento de informações sigilosas. A manutenção da improcedência do pedido reflete não apenas a rigidez judicial em casos de vazamento de dados, mas também a análise criteriosa de provas e a responsabilidade dos órgãos envolvidos.



Provedor de conexão deve fornecer dados cadastrais de usuário

A 3ª Turma do STJ decidiu que um provedor de conexão deve fornecer os dados cadastrais de um usuário somente com a indicação do IP, sem precisar da porta lógica.

O caso em questão envolve a Companhia Brasileira de Offshore (CBO), que processou a Telefônica Brasil, para obter dados de um usuário que enviou um e-mail anônimo e difamatório sobre diferenças salariais.

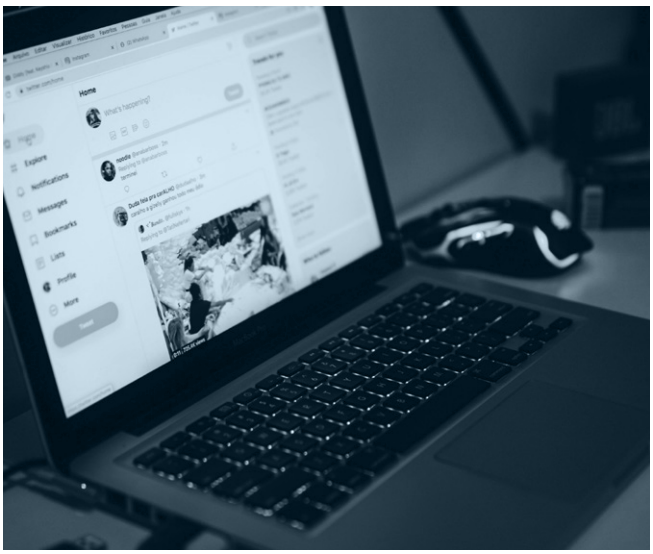
As primeira e segunda instâncias do Tribunal de Justiça de São Paulo (TJSP) decidiram a favor da CBO, mas a Telefônica alegou que não poderia compartilhar os dados por questões de sigilo cadastral, uma vez que, sem a porta lógica, haveria o fornecimento de informações de centenas de usuários que utilizaram o mesmo IP, mas não necessariamente estariam relacionados com os fatos.

No STJ, a ministra-relatora Nancy Andrighi determinou que a Telefônica compartilhasse as informações cadastrais, citando a jurisprudência que obriga tanto provedores de conexão quanto de aplicação a fornecer esses dados.

A Telefônica defende sua postura para evitar a divulgação de dados pessoais de terceiros, enquanto a CBO argumenta que o e-mail calunioso causou danos à honra dos envolvidos, solicitando o nome completo, CPF, endereço e telefone do usuário.

No voto, a ministra destacou que não é necessária a informação prévia sobre a porta lógica para que o provedor de conexão disponibilize os dados do usuário, pois ele é obrigado a armazenar e fornecer o IP e a porta lógica (Recurso Especial, REsp nº 2170872). A Turma já havia se posicionado anteriormente, ressaltando que o Marco Civil da Internet estabelece a obrigatoriedade de guardar e fornecer informações sobre a porta lógica de origem (REsp nº 1777769), e que esse armazenamento deve ocorrer pelo prazo de prescrição da ação de reparação civil de acordo com o Código Civil (REsp nº 1622483).

Sendo assim, a decisão do STJ reafirma a responsabilidade dos provedores de conexão em facilitar a identificação de usuários envolvidos em condutas ilícitas, equilibrando a proteção das informações pessoais com a necessidade de justiça em casos de difamação.



STJ livra banco de responsabilidade por "golpe do motoboy"

O STJ decidiu que um banco não pode ser responsabilizado pelo "golpe do motoboy" na ausência de provas de vazamento de dados, mesmo envolvendo uma consumidora em situação de hipervulnerabilidade. A decisão, adotada por maioria de votos, é da 3ª Turma.

No "golpe do motoboy", estelionatários se passam por representantes de instituições financeiras e informam ao cliente que seu cartão foi clonado, solicitando que um motoboy colete o cartão pessoalmente. Eles ainda pedem que o cliente digite sua senha no telefone antes da entrega.

No caso específico, a consumidora, que estava em tratamento de quimioterapia para câncer, foi enganada por golpistas que a convenceram a instalar um programa que possibilitou o acesso remoto ao seu computador. Ela também forneceu seus dados bancários e senhas, permitindo a realização de transferências fraudulentas.

O Tribunal de Justiça de Minas Gerais (TJMG) entendeu que o banco não poderia ser responsabilizado por compras realizadas com senha, uma vez que a consumidora entregou voluntariamente suas informações pessoais ao golpista, mesmo sendo vítima de estelionato.

O julgamento no STJ, iniciado em dezembro de 2024 e finalizado em fevereiro deste ano, teve como relatora a ministra Nancy Andrighi, que defendeu a responsabilidade objetiva do banco, em conformidade com a Súmula 479 do STJ. Essa súmula estabelece que instituições financeiras são responsáveis pelos danos oriundos de fraudes e delitos praticados por terceiros nas operações bancárias. A relatora foi apoiada pelo ministro Humberto Martins, mas sua posição não prevaleceu.

O ministro Ricardo Villas Bôas Cueva divergiu, argumentando que não houve falha no serviço prestado pelo banco. Ele afirmou que os golpistas agiram de forma astuta, utilizando apenas dados cadastrais da vítima. Cueva também destacou que as dificuldades enfrentadas pela consumidora em tratamento de câncer não diminuem sua responsabilidade. Os ministros Moura Ribeiro e Antônio Carlos Ferreira apoiaram a posição de Cueva, formando a maioria.

Há precedentes nas turmas de direito privado que eximem os bancos de responsabilidade quando o consumidor entrega sua senha a golpistas. Em fevereiro, a 4ª Turma manteve a decisão de um tribunal estadual que não identificou falha no serviço em operações realizadas regularmente, onde a conta foi acessada com cartão e senha fornecidos pela própria titular antes da notificação do estelionato (Agravo em Recurso Especial, AREsp nº 2756405).

Apesar disso, o tema requer monitoramento, pois esse entendimento pode mudar, e bancos poderão ser responsabilizados em casos com movimentações atípicas envolvendo suposto vazamento de dados e consumidores hipervulneráveis.

Sócias responsáveis pelo boletim

- Patrícia Helena Marta Martins
- Marcela Waksman Ejnisman
- Carla do Couto Hellu Battilana
- Luiza Sato
- Bruna Borghi Tomé
- Sofia Kilmar
- Stephanie Consonni de Schryver