TozziniFreire.

Cybernews

10ª 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 no mês de novembro de 2025.

Em primeiro lugar, trazemos uma análise sobre a proteção de dados neurais no Brasil, uma visão prática para empresas sob a ótica da legislação brasileira.

Além disso, a plataforma Reddit ajuíza ação judicial contra a startup Perplexity por coleta ilegal de dados da plataforma para treinar seu sistema de inteligência artificial, envolvendo também outras empresas na extração não autorizada de informações.

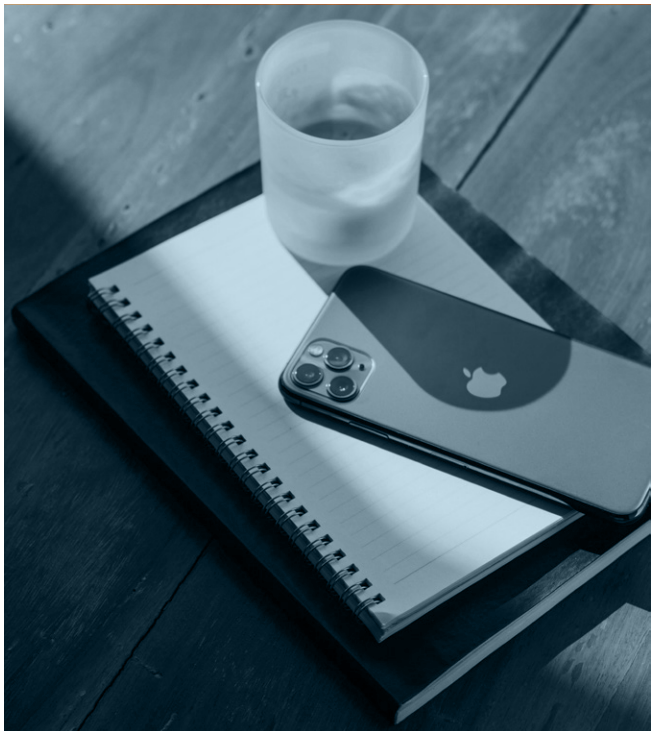
Ainda, o Tribunal de Justiça do Estado de São Paulo (TJSP) acolheu um pedido para que o X Brasil (antigo Twitter Brasil) mantivesse os dados de usuários vinculados a perfis falsos que seriam responsáveis por informações falsas.

Por fim, a 3ª Turma do Superior Tribunal de Justiça (STJ) determinou a realização de uma perícia na área de Compliance e Gestão de Riscos da PagSeguro, após alegação de uma das partes de que a credenciadora não estaria respeitando normas regulatórias e internas para verificar quem são seus clientes.

NOTÍCIAS GERAIS

Proteção de dados neurais no Brasil: visão prática para empresas sob a ótica da legislação brasileira

A popularização das interfaces cérebro-computador, dos neurodispositivos vestíveis, e das técnicas capazes de captar ou modular a atividade cerebral vem abrindo um campo de dados pessoais particularmente sensível: o de **dados neurais**. No Brasil, embora a Lei Geral de Proteção de Dados Pessoais (LGPD) não mencione "dados neurais" de forma expressa, seu conjunto de regras e princípios já oferece base consistente para orientar o tratamento e a proteção dessas informações.



Dados neurais são informações derivadas de sinais elétricos, hemodinâmicos ou de outros correlatos da atividade cerebral, captados por sensores ou inferidos por modelos algorítmicos. Seu enquadramento jurídico depende da finalidade do tratamento e da possibilidade de vinculação a uma pessoa natural identificada ou identificável. Em grande parte dos cenários práticos, esses dados se qualificam como pessoais e, com frequência, assumem natureza sensível, seja porque constituem biometria utilizada para identificação, seja por estarem associados a finalidades de saúde como diagnóstico, monitoramento ou reabilitação. O ponto de partida, portanto, deve ser a definição clara da finalidade e da natureza desses dados, considerando que mesmo sinais neurais brutos e feições derivadas podem, por sua singularidade, permitir reidentificação, o que impõe cautela específica na anonimização e na utilização de tais dados para novas finalidades.

Ao considerar as **bases legais aplicáveis ao tratamento desses dados**, o **consentimento** livre, específico e informado é a solução adequada em aplicações mais intrusivas, sobretudo quando há tomada de decisão

automatizada relevante, que exige explicação clara sobre seus efeitos. Em contextos de saúde, a LGPD admite tratamento para **tutela da saúde** por profissionais ou serviços de saúde e por autoridades sanitárias, com as devidas salvaguardas de sigilo e cautela no compartilhamento.

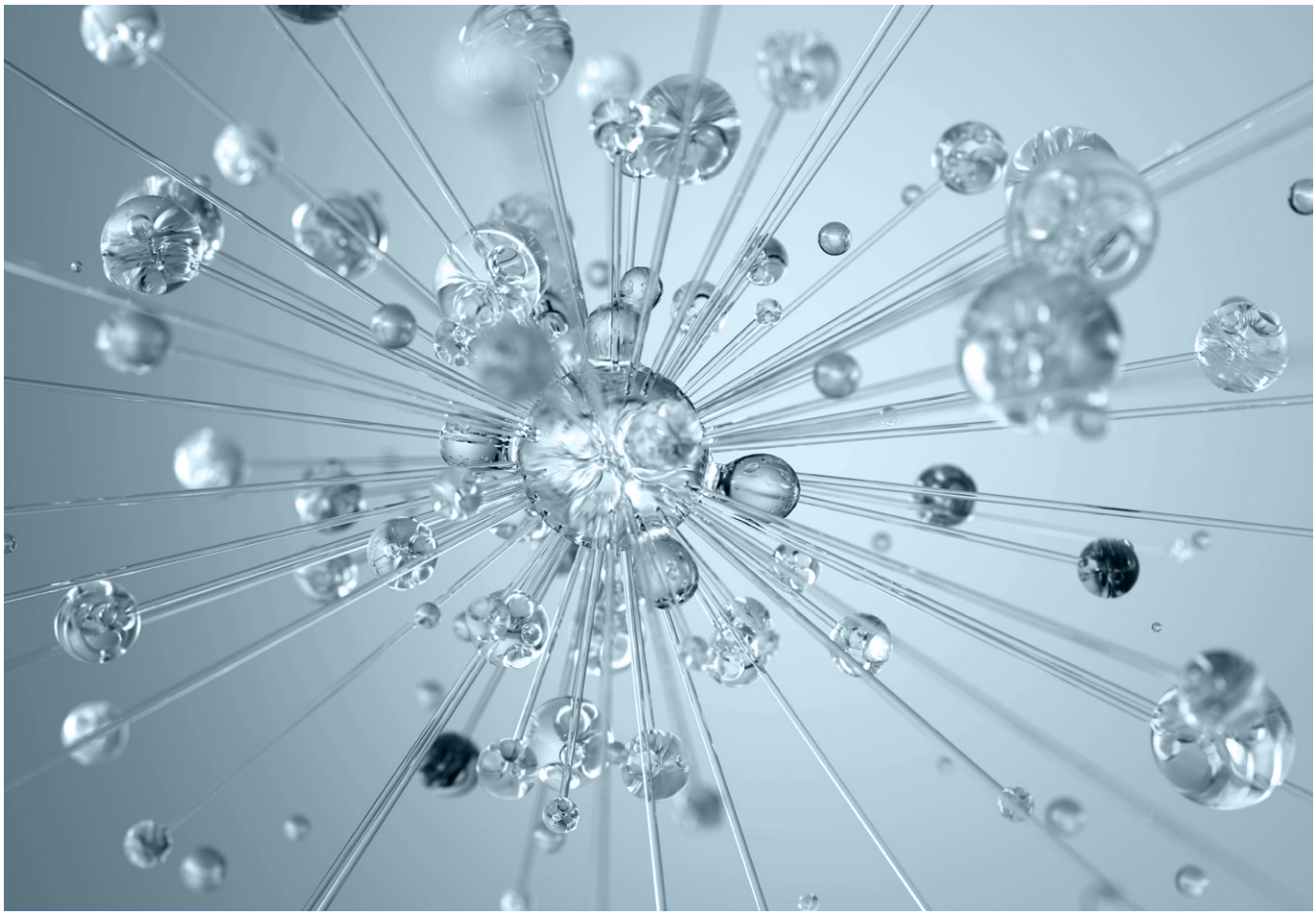
A conformidade se estrutura em torno de **princípios** que orientam qualquer operação com dados pessoais e que ganham especial relevo no universo dos neurodados. Finalidade e adequação exigem clareza sobre o propósito e coerência com o contexto de uso; necessidade e minimização sugerem coletar apenas o estritamente pertinente, privilegiando, quando cabível, o processamento local e feições derivadas em vez de sinais brutos. A transparência, por sua vez, pressupõe oferecer informações acessíveis sobre duração, agentes de tratamento, compartilhamentos e canais de atendimento, incluindo a possibilidade de revisão de decisões exclusivamente automatizadas que afetem interesses do titular. Quanto à anonimização, a avaliação técnica de risco residual e de cenários de reidentificação contribui para escolhas mais prudentes, especialmente diante de padrões neurais potencialmente únicos. Para reuso de dados, a compatibilidade com a finalidade original ou a identificação de nova base legal, acompanhada de informação prévia ao titular, promove segurança jurídica e confiança.

A governança tende a ser mais eficaz quando incorpora uma **avaliação estruturada de riscos.** Em tratamentos com potencial impacto significativo sobre liberdades civis e direitos fundamentais, os relatórios de impacto à proteção de dados atuam como instrumento de diagnóstico e de mitigação, descrevendo tipos de dados, métodos de coleta, medidas de segurança e salvaguardas organizacionais. Ademais, práticas de privacidade e segurança por desenho e por padrão, como criptografia em trânsito e em repouso, proteção de chaves, segregação de ambientes, controle granular de acesso, atualização segura de firmware e monitoramento de Interfaces de Programação de Aplicativos (APIs, na sigla em inglês), contribuem para reduzir superfícies de exposição. Em caso de incidentes com risco ou dano relevante, a comunicação ágil e clara à Agência Nacional de Proteção de Dados (ANPD) e aos titulares, indicando os dados afetados, os riscos e as providências adotadas, favorece a mitigação e o alinhamento com as expectativas regulatórias.

A análise da ANPD no **Radar Tecnológico sobre neurotecnologias** (disponível aqui) converge com esse enquadramento, oferecendo um importante parâmetro para o mercado. O documento destaca que neurodados, via de regra, comportam-se como informações de alta sensibilidade e recomenda identificar finalidades com precisão, comunicar em linguagem acessível e reconhecer os desafios na obtenção de consentimento em tecnologias complexas. Além disso, o Radar chama atenção para **riscos de reidentificação e de perfilamento, sobretudo quando há uso de inteligência artificial**, sinalizando a importância de

avaliações técnicas, governança de modelos e mitigação de vieses. Ao mapear aplicações em saúde, consumo e educação, o Radar sugere uma abordagem proporcional, com supervisão adequada e salvaguardas compatíveis com o nível de risco, visando equilibrar inovação e proteção de direitos.

Assim, um caminho possível para lidar com essa categoria de dados pessoais passa por mapear fluxos de neurodados e classificá-los conforme sua natureza (biométrica, de saúde ou inferências sensíveis), documentar finalidades e bases legais, e alinhar práticas de minimização e retenção ao ciclo de vida do produto ou serviço. A transparência, acompanhada da disponibilização de canais de exercício de direitos e de explicações sobre critérios de decisões automatizadas, contribui para os requisitos de prestação de contas. A adoção de segurança *by design*, apoiada por avaliações de risco e por relatórios de impacto quando necessário, tende a reduzir incertezas regulatórias e a facilitar o diálogo com a ANPD. Nesse cenário, a combinação entre boa engenharia de dados, governança clara e comunicação objetiva cria as condições para que projetos com neurotecnologias avancem de forma responsável.



Reddit processa Perplexity por uso indevido de dados para treinar sistema de IA

A plataforma Reddit moveu uma ação judicial contra a startup de inteligência artificial (IA) Perplexity, alegando a coleta ilegal de dados do site para treinar seu sistema de busca, o "Answer Engine". O processo, apresentado na Justiça Federal de Nova York, também envolve outras três empresas de tecnologia — Oxylabs, AWMProxy e SerpApi — que supostamente participaram da extração dos dados.

A queixa sustenta que as empresas burlaram os mecanismos de proteção do Reddit para obter informações dos subreddits sem autorização, utilizando-as para aprimorar a ferramenta de respostas automatizadas da Perplexity. O diretor jurídico do Reddit, Ben Lee, destacou que a competição por conteúdo de qualidade alimenta uma "economia de lavagem de dados".

O Reddit é conhecido por ser uma das fontes mais referenciadas em respostas geradas por sistemas de IA e possui contratos de licenciamento com grandes empresas como Google e OpenAI. A Perplexity, por sua vez, negou as irregularidades e se comprometeu a defender a inovação aberta em sua abordagem.

A SerpApi também se defendeu contra as acusações, enquanto a Oxylabs expressou surpresa com a ação judicial, alegando que não houve tentativa de diálogo prévio. O processo requer indenização financeira não especificada e uma ordem judicial para impedir o uso contínuo dos dados do Reddit pela Perplexity.

Esse caso ressalta a importância da proteção de dados pessoais no ambiente das tecnologias emergentes, onde a utilização não autorizada de informações pode comprometer tanto a competitividade quanto a integridade das plataformas.

Justiça de SP determina a preservação da identidade de perfis para coibir fakes no X Brasil

O Tribunal de Justiça de São Paulo (TJSP) acatou o pedido de liminar do Sleeping Giants, determinando que a plataforma X (antigo Twitter) mantenha registros dos endereços de IP utilizados por perfis que realizam denúncias falsas. Esses endereços funcionam como uma identificação única das máquinas em uso.

A ação judicial foi ajuizada sob a alegação de aumento de perfis falsos que abusam de nomes de jornalistas e entidades, fazendo denúncias inverídicas, especialmente contra políticos de esquerda e meios de comunicação. O Sleeping Giants defendeu que a plataforma X retenha os registros desses perfis a fim de facilitar ações judiciais e pedidos de indenização.

Importante ressaltar que uma das contas responsáveis por denúncias falsas já foi suspensa após a propagação de mais de 1.500 mensagens enganosas.

Em um contexto em que a desinformação se espalha rapidamente por meio das redes sociais, a decisão do TJSP destaca a relevância da proteção de dados pessoais. A preservação da identidade dos perfis envolvidos em atividades fraudulentas é um passo essencial para garantir a responsabilização e integrar um ambiente de informações mais seguro e confiável.

STJ determinou que fosse realizada perícia em caso de fraude bancária envolvendo PagSeguro

A 3ª Turma do Superior Tribunal de Justiça (STJ) determinou a realização de perícia na área de compliance e gestão de riscos da PagSeguro em resposta a um caso de fraude bancária. O pedido, realizado pelo Santander, surge após o banco ter arcado com os prejuízos provenientes de uma transação fraudulenta.

Esse desdobramento é significativo, pois estabelece um importante precedente no STJ, que até então se concentrava em conflitos judiciais entre consumidores e lojistas contra instituições financeiras. Nessa ocasião, um banco moveu uma ação contra uma credenciadora, questionando a responsabilidade civil pela fraude e alegando que a PagSeguro não estaria cumprindo as normas regulatórias e internas necessárias para a verificação de seus clientes.

O caso analisado envolve o uso de conta fraudulenta feita por golpistas no Santander, aberta com documentos falsos, com o intuito de transferir dinheiro para um suposto estabelecimento comercial, por meio da PagSeguro. Alega-se que os acusados tomavam empréstimos junto ao banco e desviavam benefícios do INSS, repassando valores para uma loja credenciada da empresa de maquininha de cartão. Foram desviados R$ 40,7 mil.

O banco assumiu o prejuízo, mas entrou com ação contra a PagSeguro para pedir a responsabilidade. Em termos financeiros, segundo especialistas, a ação não teria tanta repercussão, mas seria importante pela tese, pois situações como essa são recorrentes para as instituições financeiras. Até então, as decisões foram desfavoráveis ao banco.

No contexto atual, a decisão do STJ reflete uma crescente preocupação com a segurança no sistema de pagamentos, especialmente diante da ascensão dos golpes digitais. Esse reconhecimento judicial pode estabelecer um precedente crucial que incentive as instituições financeiras a reforçarem seus sistemas de prevenção contra fraudes, protegendo assim melhor seus clientes e promovendo um ambiente mais seguro nas transações financeiras.

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