TozziniFreire.

Cybernews

1ª Edição | 2026

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 o debate de proteção de dados perante os Tribunais no mês de janeiro de 2026.

Em primeiro lugar, os cartórios de notas do país lançaram a ferramenta e-Not Provas, que permite registrar conteúdos digitais, como postagens em redes sociais e mensagens em aplicativos, conferindo-lhes validade jurídica. Com a supervisão de tabeliães de notas, o serviço assegura a integridade das provas em um ambiente seguro, atendendo a crescentes demandas no contexto digital. A iniciativa moderniza o Direito, possibilitando a utilização de provas digitais em processos judiciais e administrativos.

Recentemente, o Tribunal Superior do Trabalho (TST) definiu que a geolocalização pode ser usada como prova digital em demandas trabalhistas que envolvam pedidos de horas extras, desde que em conformidade com os limites de privacidade e sigilo.

Além disso, ocorreu no início deste ano a abertura de inquérito pelo ministro Alexandre de Moraes, do Supremo Tribunal Federal (STF), para apurar um possível vazamento de dados de ministros da Corte, oriundos da Receita Federal e do Conselho de Controle de Atividades Financeiras (Coaf).

Ademais, o Instituto de Defesa do Consumidor (Idec) denunciou a ferramenta Grok, inteligência artificial da plataforma X, à Agência Nacional de Proteção de Dados (ANPD) por modificar imagens de pessoas reais, incluindo crianças, de forma sexualizada e sem consentimento.

A Airbnb Plataforma Digital Ltda. foi condenada ao pagamento de indenização de R$ 6 mil por danos morais, em decorrência da invasão de um terceiro em um apartamento alugado pela plataforma.

Por fim, confira o Mapa de Temas Prioritários para o biênio 2026-2027 e atualização da Agenda Regulatória 2025-2026 da ANPD.

NOTÍCIAS GERAIS

Cartórios de notas inauguram o chamado "e-Not Provas"

Recentemente, os cartórios de notas lançaram a inovadora ferramenta e-Not Provas, que revoluciona a forma como atualmente se lida com a produção de provas sobre conteúdos disponíveis na internet.

A ferramenta e-Not Provas oferece um serviço digital que permite registrar informações publicadas em sites, mensagens trocadas em aplicativos e postagens em redes sociais, conferindo validade jurídica a esses conteúdos. Com a presença de um tabelião de notas, responsável por garantir a fé pública, a integridade das informações registradas é assegurada em um ambiente virtual controlado, prevenindo qualquer alteração ou interferência externa durante o processo de coleta. Este aspecto é crucial, pois garante que a autenticidade das provas esteja preservada ao longo do tempo.

Na era da informação, onde disputas e litígios muitas vezes giram em torno de elementos virtuais, a função do e-Not Provas se torna ainda mais evidente. Esse serviço atende não só a indivíduos, mas também a empresas e profissionais do Direito que precisam validar a existência e a apresentação de determinados conteúdos em momentos específicos. A coleta é feita em um ambiente isolado e seguro, onde a privacidade do usuário é respeitada e protegida.

Além da inovação técnica, a ferramenta gera códigos hash criptográficos, que garantem a integridade das provas, reforçando a confiabilidade do material produzido.

Com valores acessíveis, que correspondem à autenticação notarial, e armazenamento por até cinco anos, essa ferramenta é uma resposta ágil e eficaz às necessidades de demandas que exigem a interface entre o Direito e a evolução das tecnologias.

TST permitiu a adoção de geolocalização em processos trabalhistas para apuração de horas extras

O Tribunal Superior do Trabalho (TST) decidiu que empresas podem utilizar dados de geolocalização – tecnologia que identifica a localização geográfica de uma pessoa por meio de GPS, Wi-Fi ou redes de celular – como prova em demandas trabalhistas que envolvam pedidos de horas extras.

Nos dois casos analisados, de um propagandista vendedor e outro de uma bancária, o TST entendeu que a geolocalização é um meio válido para verificar a jornada de trabalho, desde que respeitados limites de privacidade e sigilo.

A decisão em comento foi tomada pela Subseção II Especializada em Dissídios Individuais e pela 5ª Turma do TST, as quais consideraram a referida prova precisa, necessária e proporcional, dentro do que dispõe a Lei Geral de Proteção de Dados (LGPD) e o Marco Civil da Internet (MCI), que admitem a utilização de dados pessoais para o exercício regular do direito em processo judicial.

Registraram, ainda, que a geolocalização nesses casos não viola o direito fundamental à privacidade, previsto na Constituição Federal, mas que o seu uso deve se restringir efetivamente ao período contratual e aos horários alegados pelo trabalhador, além disso, os processos que utilizarem esse mecanismo devem tramitar em segredo de justiça para garantir a proteção das informações.

Segundo o TST, a geolocalização não viola a intimidade nem o sigilo telemático dos empregados, representando um avanço significativo na aceitação de provas digitais em disputas trabalhistas.

Ministro Alexandre Moraes abre inquérito para apurar vazamento de dados de ministros do STF

Em janeiro de 2026, o Brasil vivenciou um episódio que ressalta a importância da proteção de dados pessoais: o ministro Alexandre de Moraes, do Supremo Tribunal Federal (STF), abriu um inquérito para investigar um possível vazamento de dados de ministros da Corte, provenientes da Receita Federal e do Coaf. Esse caso envolve a suspeita de quebra irregular de sigilo fiscal, levantando questões sobre a responsabilidade na utilização de informações sensíveis.

A LGPD no Brasil requer que o tratamento de dados pessoais seja transparente e realizado com consentimento adequado. O acesso da Receita Federal e do Coaf a essas informações exige autorização judicial, especialmente considerando a privacidade das pessoas envolvidas, como familiares dos ministros.

A investigação, conduzida pela Polícia Federal, reforça a necessidade de controle rigoroso sobre o uso de informações protegidas, de modo a evitar danos irreparáveis. O papel das instituições governamentais na salvaguarda dos dados que administram deve ser prioridade, especialmente em investigações com implicações políticas e sociais.

Além do setor público, empresas privadas devem implementar práticas eficazes de governança de dados, garantindo conformidade com as regulamentações. Isso inclui auditorias regulares e treinamentos sobre privacidade de dados.

O inquérito do STF é um lembrete da centralidade da proteção de dados na era digital. É essencial que todos — indivíduos e instituições — adotem práticas robustas para garantir a conformidade legal e o respeito aos direitos fundamentais. A transparência e a segurança na gestão da informação são essenciais para manter a confiança pública.

Idec denuncia Grok à ANPD por modificação sexualizada de imagens de pessoas reais

No dia 14 de janeiro de 2026, o Instituto de Defesa do Consumidor (Idec) apresentou uma denúncia à Agência Nacional de Proteção de Dados (ANPD), requerendo a investigação da ferramenta Grok – inteligência artificial integrada à plataforma *X* – e a imposição de restrições ao seu uso em todo o território nacional.

De acordo com o Idec, a Grok teria violado reiteradamente a LGPD ao gerar imagens sexualizadas preservando características reais de pessoas retratadas, inclusive crianças e adolescentes, sem qualquer forma de consentimento. Usuários estavam utilizando a IA para modificar fotos de indivíduos reais, com *prompts* instruindo a ferramenta a despir a pessoa da imagem ou colocá-la em roupas reveladoras.

Entre os pedidos formulados, o instituto requer a suspensão imediata de todas as funcionalidades da Grok relacionadas ao tratamento de dados pessoais. O Idec também solicita que as violações sejam investigadas, que a ANPD adote medidas urgentes para prevenir ou reparar danos graves e que a plataforma *X* preste esclarecimentos sobre o caso.

O instituto destaca ainda que a geração desse tipo de conteúdo pela Grok tem sido alvo de investigações e sanções por autoridades da Califórnia, União Europeia, Reino Unido, Índia, dentre outras jurisdições, tratando-se de um problema "*sistêmico e global*".

Na mesma data, a plataforma *X* anunciou a adoção de medidas para bloquear, em determinadas jurisdições, a capacidade da Grok de modificar fotos para gerar imagens de pessoas usando "*biquínis, roupas íntimas e outras peças similares*".

O episódio evidencia a tensão persistente entre o avanço das tecnologias de IA e a necessidade de resguardar direitos assegurados pelo ordenamento jurídico brasileiro, como a proteção de dados pessoais, a tutela da infância e a inviolabilidade da intimidade, honra e imagem.

Senha igual: Airbnb indenizará por entrada de terceiro em apartamento alugado com uso de fechadura eletrônica

A 1ª Turma Recursal dos Juizados Especiais do Tribunal de Justiça do Estado do Paraná (TJPR) condenou a Airbnb Plataforma Digital Ltda. ao pagamento de R$ 6 mil por danos morais, em decorrência da invasão de um terceiro em um apartamento alugado pela plataforma.

O incidente ocorreu quando dois hóspedes reservaram um apartamento pelo Airbnb e, no segundo dia da estadia, um estranho conseguiu acessar o imóvel por meio da fechadura eletrônica. Ao reportar a situação ao anfitrião, os hóspedes foram informados de que havia ocorrido uma confusão quanto ao número do apartamento reservado, sendo que o anfitrião também alugava outra unidade no mesmo prédio.

Embora o pedido de indenização por danos morais tenha sido inicialmente negado em 1ª instância, o TJPR reformou essa decisão ao avaliar o caso. O relator, juiz Douglas Marcel Peres, rejeitou a justificativa do anfitrião, ressaltando que a adoção de uma única senha para diferentes unidades no mesmo edifício compromete a segurança e a privacidade dos hóspedes.

O magistrado enfatizou que a expectativa básica ao reservar uma hospedagem é ter segurança no local e denunciou a prática da senha única como um risco claro de invasões por terceiros.

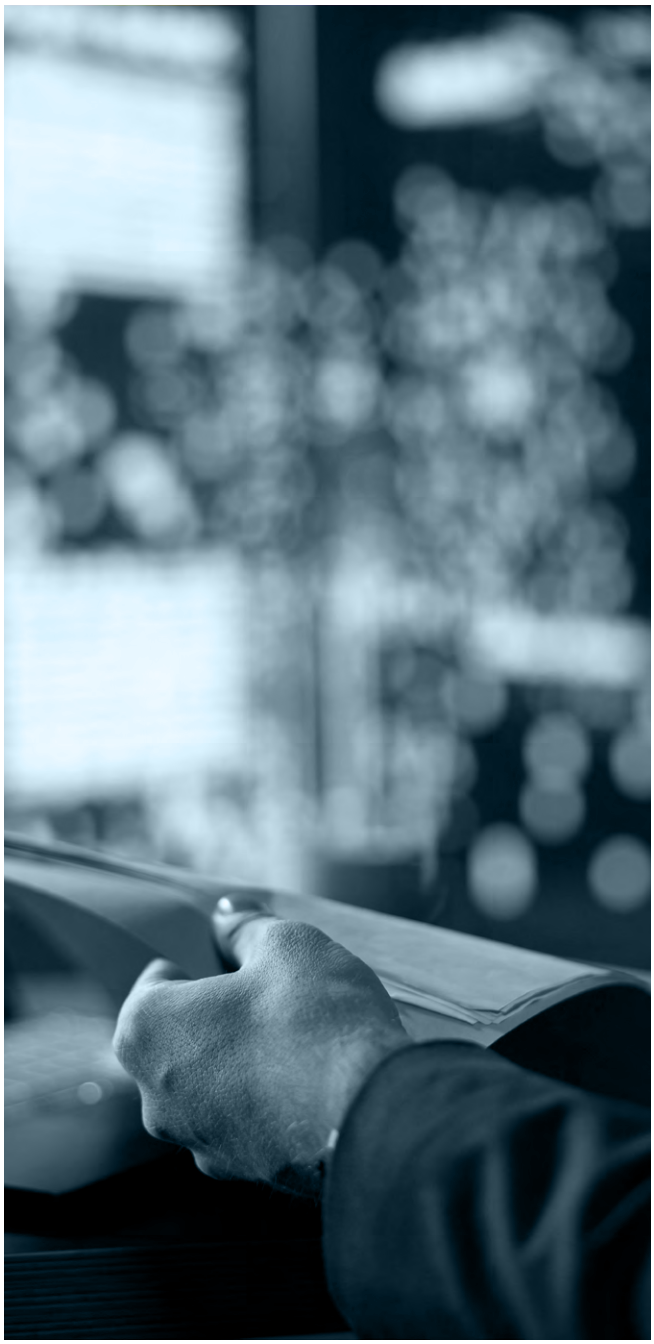
Por fim, essa situação destaca a necessidade crítica de medidas robustas de proteção de dados e privacidade nas plataformas digitais.

A expectativa de segurança é primordial para os consumidores, e os prestadores de serviços devem implementar protocolos de segurança eficazes para proteger as informações e propriedades dos usuários.

Discutir a privacidade e a proteção de dados, especialmente em incidentes como este, é essencial para construir confiança na economia compartilhada e assegurar a segurança de todos os envolvidos.

ANPD EM FOCO

Mapa de Temas Prioritários para o biênio 2026-2027 e atualização da Agenda Regulatória 2025-2026 da ANPD



Em 24 de dezembro de 2025, a ANPD publicou duas resoluções que orientam sua atuação nos próximos ciclos: Resolução CD/ANPD nº 30/2025 (veja aqui), que define o Mapa de Temas Prioritários de Fiscalização para o biênio 2026-2027, e a Resolução CD/ANPD nº 31/2025 (veja aqui), que atualizou a Agenda Regulatória para o biênio 2025-2026.

A publicação conjunta dessas resoluções reforça uma **estratégia integrada de regulamentação e fiscalização**, que envolverão o monitoramento, orientação e atuação preventiva da ANPD, de assuntos relacionados à proteção de dados e à Lei nº 15.211/2025 (Estatuto da Criança e do Adolescente Digital – ECA Digital).

Veja abaixo um resumo dos principais tópicos apresentados no Mapa de Temas Prioritários e Agenda Regulatória da ANPD:


1º sem/2026
2º sem/2026
1º sem/2027
2º sem/2027
Regulamentação
IA: 20 fiscalizações em tecnologias emergentes, especialmente sistemas de IA
Tratamento pelo Poder Público: +20 fiscalizações de adequação do Poder Público
Proteção de crianças e adolescentes no ambiente digital: +30 fiscalizações sobre adequação às exigências do ECA Digital
Direitos dos titulares: 10 fiscalizações relacionados a dados biométricos, de saúde ou financeiros
Direitos dos titulares: 25 fiscalizações de temas diversos + 5 de uso secundário de dados para publicidade
Fiscalização
1. Direitos dos titulares
2. RIPD
3. Compartilhamento de dados pelo Poder Público
4. Dados biométricos
5. Medidas de segurança
6. IA
7. Anonimização e pseudonimização
1. Agregadores de dados pessoais
2. Dados de saúde
3. Guia orientativo sobre escopo e obrigações gerais do ECA Digital (fornecedores de produtos ou serviços de TI)
4. Fiscalização e Sanção do ECA Digital - Revisão das Resoluções CD/ANPD nº 1/2021 e nº 4/2023
5. Mecanismos de aferição de idade
1. Processo normativo no âmbito da ANPD: revisão da Portaria nº 16/2021
1. Regras de boas práticas e de governança
2. Hipótese Legal do consentimento e proteção ao crédito

O **Mapa de Temas Prioritários** prevê quatro temas prioritários para a atividade de fiscalização da ANPD no biênio 2026-2027, com metas e cronogramas semestrais específicos para cada tema:

i. direitos dos titulares, especialmente quanto ao tratamento de dados biométricos, de saúde e financeiros;

ii. proteção de crianças e adolescentes no ambiente digital;

iii. tratamento de dados pessoais pelo Poder Público; e

iv. inteligência artificial e tecnologias emergentes no contexto do tratamento de dados pessoais.

Esses temas foram definidos a partir da análise de informações obtidas com requerimentos, comunicações de incidentes e ações de fiscalização nos últimos dois anos.

Já a **Agenda Regulatória 2025-2026** foi atualizada para incluir novos itens diretamente ligados ao ECA Digital, além de aperfeiçoamentos transversais no processo normativo e a manutenção de temas previamente previstos:

i. mecanismos de aferição de idade;

ii. guia orientativo sobre o escopo e obrigações gerais do ECA Digital para fornecedores de produtos ou serviços de TI; e

iii. revisão das resoluções sancionatórias nº 1/2021 e nº 4/2023 à luz do ECA Digital.

Para o setor privado, a tendência é de intensificação da atuação fiscalizatória e sancionatória sobre direitos dos titulares, em especial crianças e adolescentes, dados sensíveis (biometria, saúde e financeiro), publicidade direcionada baseada em uso secundário e medidas de adequação ao ECA Digital, exigindo revisões de bases legais, minimização e governança de dados. No campo de **inteligência artificial**, espera-se amadurecimento regulatório e testes de conformidade com foco em decisões automatizadas e riscos a grupos vulneráveis.

No setor público, 2027 trará um ciclo de 20 fiscalizações e monitoramento do uso compartilhado de dados pessoais, pressionando por conformidade com salvaguardas técnicas e legais.

Sócias responsáveis pelo boletim

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