

TozziniFreire.

# Cybernews

---

5ª Edição | 2025

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

# SUMÁRIO

Clique na notícia e navegue  
pelo documento 

## 01 INTRODUÇÃO

---

## 02 NOTÍCIAS GERAIS

---

Reconhecimento facial e dados biométricos: os riscos e as respostas da ANPD

Tribunal Regional do Trabalho da 7ª Região impõe multa por litigância de má-fé e remete caso à OAB devido ao uso suspeito de IA

Tribunal de Justiça de Santa Catarina nega pedido a parte que usou vídeo editado por IA como prova

STJ entende pela manutenção de plataforma que oferece a elaboração de petições iniciais por meio de IA

Empresa de Bitcoin responde por danos causados por fraude em transação

# INTRODUÇÃO

---

Nesta edição do Cybernews, destacamos as principais notícias sobre proteção de dados no mês de junho de 2025.

Confira nossa opinião sobre o reconhecimento facial e dados biométricos relacionados aos riscos e as respostas da Autoridade Nacional de Proteção de Dados (ANPD).

Além disso, trazemos a decisão do Tribunal Regional do Trabalho da 7ª Região (TRT7) que não conheceu um recurso ordinário devido à ausência de dialeticidade e à apresentação de jurisprudência manipulada em virtude da suspeita de uso de ferramentas de inteligência artificial (IA). Foi aplicada multa por litigância de má-fé e determinado o envio de ofício à Ordem dos Advogados do Brasil (OAB) para apuração de possível infração disciplinar.

Ainda, foi proferida decisão por desembargador que negou um pedido judicial baseado em um vídeo editado por IA, apresentado como prova em um concurso público.

O Superior Tribunal de Justiça (STJ) decidiu manter o funcionamento da plataforma “Resolve Juizado”, que oferece a elaboração de petições iniciais com o auxílio de inteligência artificial por R\$ 19,90.

Por fim, a 4ª Turma do STJ condenou uma plataforma de investimentos digitais em criptomoedas a indenizar um usuário que foi vítima de fraude, sob o entendimento de que as instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a fraude praticada por terceiros em operações bancárias.

# NOTÍCIAS GERAIS

## Reconhecimento facial e dados biométricos: os riscos e as respostas da ANPD

O uso de ferramentas baseadas em reconhecimento facial tem se tornado cada vez mais presente no cotidiano brasileiro. Atualmente é comum encontrá-las não apenas no desbloqueio de dispositivos móveis e no controle de acesso a prédios, mas também em sistemas de autenticação financeira, em estádios de futebol e em programas de vigilância urbana.

Esse avanço, contudo, é acompanhado por uma preocupação crescente: o tratamento de dados biométricos, que são classificados como dados pessoais sensíveis de acordo com a Lei Geral de Proteção de Dados Pessoais (LGPD). Por sua natureza única, imutável e altamente identificável, dados de biometria facial, impressões digitais, voz e íris demandam um nível elevado de cuidado e proteção. O uso inadequado desses dados pode gerar impactos significativos para os titulares.

Nesse contexto, a Autoridade Nacional de Proteção de Dados (ANPD) vem se posicionando de forma cada vez mais ativa, com o objetivo de orientar o mercado e estruturar salvaguardas jurídicas e técnicas em torno do uso de tecnologias biométricas.

Em 2024, a ANPD já havia publicado um estudo preliminar sobre “Biometria e Reconhecimento Facial”. Entre os pontos destacados, a autoridade alertava para a aplicação de tecnologias em contextos sensíveis, como segurança pública, escolas e consumo. Além disso, foi ressaltada a necessidade de transparência, com bases legais claras e o uso adequado do consentimento. O documento também chamava atenção para os riscos de vieses algorítmicos, que podem reproduzir discriminações raciais, sociais ou econômicas, bem como para a coleta não informada, que impede o exercício dos direitos dos titulares e compromete a validade jurídica do tratamento.

No começo deste ano, esse posicionamento ganhou contornos mais concretos com a decisão da ANPD no caso da Tools for Humanity, empresa responsável pelo projeto World ID. A autoridade determinou a suspensão da oferta de pagamentos e recompensas em troca da coleta de dados biométricos. De acordo com a autoridade, esse tipo de incentivo compromete a liberdade de escolha dos titulares e torna inválido o consentimento, especialmente em contextos que envolvem

populações em situações de vulnerabilidade. A ANPD também exigiu que a empresa disponibilizasse informações claras sobre o encarregado de dados, no Brasil, reforçando seu compromisso com a efetiva responsabilização dos agentes de tratamento.

Mais recentemente, em junho de 2025, a ANPD deu mais um passo importante ao lançar uma Tomada de Subsídios sobre “Tratamento de Dados Pessoais Sensíveis – Dados Biométricos”. A consulta, aberta ao público até o começo de julho, busca ouvir a sociedade civil, especialistas e o setor privado para subsidiar uma futura regulamentação.

A consulta está organizada em blocos temáticos que tratam de questões fundamentais, como definições técnicas, hipóteses legais de tratamento, governança, medidas de segurança da informação, proteção de grupos em situação de vulnerabilidade e impactos de tecnologias emergentes. Com esse novo passo, a ANPD tem por objetivo garantir que a regulação acompanhe a sofisticação dos usos potenciais desse tipo de dado, sem comprometer os direitos fundamentais dos titulares.

Nesse cenário, é importante que empresas e instituições que tratam dados biométricos, direta ou indiretamente, estejam atentas às expectativas já consolidadas pela ANPD. Mesmo antes da publicação de uma norma específica, já é possível identificar diretrizes que devem orientar o desenvolvimento e a contratação de soluções que envolvam reconhecimento facial ou outros sistemas biométricos.

Entre outros aspectos, é importante que o tratamento esteja respaldado em uma base legal válida, com finalidades legítimas, proporcionais e devidamente informadas aos titulares. Além disso, é recomendado a elaboração de Relatórios de Impacto à Proteção de Dados (RIPDs), em razão do tratamento de dados biométricos, especialmente em contextos de maior potencial de risco. Dessa forma, a ANPD reforça que a coleta de dados biométricos deve ser transparente e os titulares devem ter as ferramentas necessárias para compreender como seus dados estão sendo tratados, por quanto tempo e com que finalidade.

Vale ressaltar que a segurança da informação passa a ser um ponto central neste debate. Dados biométricos exigem a adoção de padrões mais elevados de proteção para assegurar um devido monitoramento contínuo de riscos.

Embora o tema esteja em processo de consolidação normativa no Brasil, a atuação recente da ANPD já fornece um conjunto robusto de orientações que já podem ser implementadas, desde já, pelas organizações. A adoção de tecnologias de biometria, se conduzida com responsabilidade e fundamentada em uma avaliação criteriosa de riscos, pode trazer ganhos significativos em segurança e eficiência. Em contrapartida, seu uso indiscriminado, sem as devidas salvaguardas jurídicas e técnicas, pode resultar em exposições relevantes, tanto do ponto de vista regulatório quanto reputacional. Nesse contexto, surge a necessidade de alinhar a inovação tecnológica à governança de dados, assegurando o respeito aos direitos dos titulares e a conformidade com a LGPD desde a concepção das soluções.

## Tribunal Regional do Trabalho da 7ª Região impõe multa por litigância de má-fé e remete caso à OAB devido ao uso suspeito de IA

A 3ª Turma do Tribunal Regional do Trabalho (TRT) da 7ª Região, por unanimidade, decidiu não conhecer o recurso ordinário em um processo trabalhista, em razão da apresentação de jurisprudência manipulada, com indícios de uso de ferramentas de inteligência artificial (IA).

Durante a análise, o TRT identificou que as alegações do reclamante eram genéricas e não contestavam os fundamentos da sentença. Além disso, o advogado do reclamante apresentou julgados inexistentes ou com dados adulterados, visando induzir o Tribunal a erro.

Em decorrência da gravidade dessa conduta, foi imposta uma multa de 2% sobre o valor atualizado da causa, e determinado o envio

de ofício à Ordem dos Advogados do Brasil (OAB) – Seccional do Ceará, para investigar uma possível infração disciplinar do advogado.

Essa decisão ressalta a relevância da ética e da boa-fé no exercício da advocacia. O desembargador relator Carlos Rebonatto destacou que a manipulação de jurisprudência compromete a integridade do sistema judiciário e viola princípios éticos fundamentais da profissão.

Esse caso estabelece um precedente significativo na defesa da transparência e responsabilidade no âmbito jurídico, enfatizando a importância do advogado na administração da justiça e o uso consciente de ferramentas de IA como apoio à prática advocatícia.



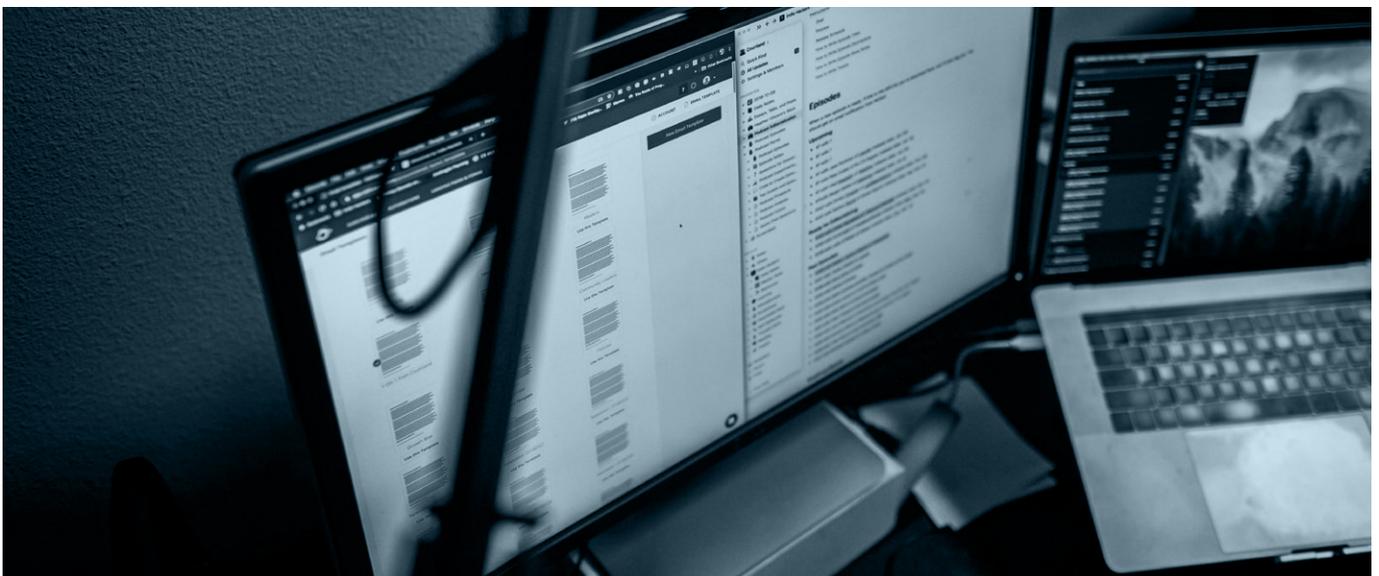
## Tribunal de Justiça de Santa Catarina nega pedido a parte que usou vídeo editado por IA como prova

O desembargador Alexandre Moraes da Rosa, do Tribunal de Justiça de Santa Catarina (TJSC), rejeitou o pedido de tutela provisória de uma candidata ao concurso da Polícia Militar, que alegou ter sido reprovada injustamente na prova de corrida. Para comprovar que cumpriu o tempo mínimo, apresentou um vídeo editado com um cronômetro digital gerado pelo ChatGPT. O magistrado considerou o material insuficiente para validar sua alegação, pois não atendia aos requisitos técnicos mínimos para ser aceito como prova pericial.

A candidata argumentou que a avaliação manual da banca poderia conter falhas, justificando a edição do vídeo. No entanto, o desembargador afirmou que o vídeo não foi autenticado por laudo técnico especializado e não continha elementos exigidos por normas técnicas, como hash criptográfico,

certificação digital, logs de software ou cadeia de custódia. Ele ressaltou que a inserção de marcações em vídeo com IA deve respeitar padrões técnicos previstos em normas como da Associação Brasileira de Normas Técnicas (ABNT) ISO/IEC 27.001, 42.001:2024 e NBR 10.520/2023, que tratam de segurança da informação, gestão de IA e documentação de fontes. Assim, a produção de prova particular pressupõe o preenchimento mínimo dessas diretrizes técnicas para garantir rastreabilidade pericial e judicial.

O desembargador também destacou o atraso de 16 meses entre a reprovação e a ação judicial, o que comprometia a urgência do pedido. A decisão não implica reprovação definitiva, mas a inviabilidade de concessão de liminar com base em provas não submetidas ao contraditório e sem respaldo técnico, recomendando perícia durante o processo.



## STJ entende pela manutenção de plataforma que oferece a elaboração de petições iniciais por meio de IA

O presidente do Superior Tribunal de Justiça (STJ), ministro Herman Benjamin, decidiu manter o funcionamento da plataforma “Resolve Juizado”, que oferece a elaboração de petições iniciais com o auxílio de IA por R\$ 19,90. A OAB-RJ havia solicitado a suspensão do serviço, alegando que ele mercantiliza a advocacia e capta clientela de forma indevida, mas o ministro discordou, afirmando que a utilização da tecnologia amplia o acesso à justiça.

Na sua análise, o ministro ressaltou que o uso de IA na elaboração de petições não configura uma afronta à legislação, pois a ferramenta visa ajudar cidadãos a formalizar suas demandas em Juizados Especiais, onde

a presença de um advogado não é obrigatória. Ele enfatizou que a decisão anterior do Tribunal Regional Federal (TRF) da 2ª Região, que permitiu a continuidade do serviço, foi acertada, já que não havia evidências concretas da irregularidade alegada pela OAB-RJ.

Com isso, a OAB-RJ informou que planeja recorrer da decisão. A controvérsia começou a partir de uma ação civil pública da OAB-RJ contra a plataforma, que foi aconselhada a suspender suas atividades em primeira instância. Entretanto, o TRF reverteu essa decisão, comparando a atuação do site a serviços em outras áreas que não configuram exercício ilegal da profissão.



## Empresa de Bitcoin responde por danos causados por fraude em transação

A 4ª Turma do STJ condenou uma plataforma de investimentos digitais em criptomoedas a indenizar um usuário que foi vítima de fraude, sob o fundamento de que as instituições financeiras, incluindo aquelas que comercializam Bitcoin, são objetivamente responsáveis pelos danos gerados por fortuito interno relacionado a fraudes praticadas por terceiros em operações bancárias.

No caso, a fraude ocorreu quando hackers acessaram o sistema da empresa durante a tentativa do usuário de transferir valores para outra corretora. A ministra relatora Isabel Gallotti entendeu que a plataforma de investimentos digitais se enquadra no conceito de instituição financeira, conforme o artigo 17 da Lei nº 4.595/1964, que a define como aquelas que têm como atividade principal ou acessória a custódia de valor de propriedade de terceiros.

Além disso, não foi constatado que os usuários tenham fornecido informações pessoais a fraudadores. Contudo, o tribunal identificou uma falha na prestação de serviços devido à falta de ferramentas de segurança adequadas para combater ataques cibernéticos, o que ensejou a responsabilização da plataforma.

A Turma, de forma unânime, acompanhou o posicionamento da relatora.

Essa decisão pode vir a se tornar paradigma em casos similares para responsabilizar plataformas de criptomoedas pela falha em implementar medidas de segurança robustas para proteger os usuários contra fraudes. Assim, é importante que as empresas que atuam nesse setor realizem auditorias de segurança regulares, invistam em tecnologias avançadas de cibersegurança e garantam conformidade com as regulamentações financeiras relevantes. Ao abordar proativamente esses riscos, elas podem mitigar sua responsabilidade e aumentar a confiança dos usuários em seus serviços.





## 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