TozziniFreire.

Cybernews

6ª 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 julho de 2025.

Um estudo recente revelou um crescimento de 112% nas decisões judiciais que mencionam a Lei Geral de Proteção de Dados (LGPD) nos tribunais brasileiros. O estudo indica que a lei está sendo cada vez mais compreendida e utilizada pelo Poder Judiciário e pelos cidadãos na busca por seus direitos, e reflete uma consolidação da cultura de proteção de dados pessoais no Brasil.

Já o Ministério da Justiça formalizou uma recente Portaria, publicada em 30 de junho de 2025, autorizando o uso de inteligência artificial (IA) com reconhecimento facial à distância em investigações criminais.

Em adição, o Superior Tribunal de Justiça (STJ) decidiu que plataformas de criptomoedas são responsáveis por fraudes em seus sistemas, mesmo quando utilizam autenticação em dois fatores. A decisão foi tomada após um investidor ter prejuízo com a transferência indevida de bitcoins, e a Corte entendeu que a falha na segurança da plataforma justifica o dever de indenização.

Por fim, o Tribunal Regional do Trabalho da 15ª região decidiu proibir a utilização de dados de geolocalização em processo trabalhista para proteger a privacidade da trabalhadora envolvida. O Tribunal destacou que a requisição de dados de geolocalização poderia violar a privacidade da parte reclamante e atrasar o processo sem garantir a utilidade necessária.

NOTÍCIAS GERAIS

Decisões que citam LGPD dobraram em um ano, aponta relatório

Um estudo recente revelou um aumento significativo nas decisões judiciais que mencionam a Lei Geral de Proteção de Dados (LGPD) nos tribunais brasileiros. Entre outubro de 2023 e outubro de 2024, foram identificadas 15.921 decisões que citam a LGPD, marcando um crescimento de 112% em relação ao período anterior, que contabilizou 7.503 decisões. O relatório, elaborado pelo Centro de Direito, Internet e Sociedade (Cedis-IDP) em parceria com o Jusbrasil e com o apoio do Programa das Nações Unidas para o Desenvolvimento (PNUD Brasil), foi apresentado em um evento prévio ao XIII Fórum de Lisboa.

Segundo Laura Schertel Mendes, diretora do Cedis-IDP, os dados indicam um amadurecimento na aplicação da LGPD pelo Judiciário. A legislação, que entrou em vigor em 2020, está sendo cada vez mais compreendida e utilizada pelos cidadãos na busca por seus direitos. Isso porque a LGPD não proíbe o uso de dados pessoais, mas regula sua governança e limites, o que tem se tornado mais claro ao longo do tempo.

Além do aumento no número de citações, as decisões que mencionam a LGPD também estão se aprimorando tecnicamente, revelando uma evolução no conhecimento do Judiciário sobre a aplicação da lei. Também merece destaque a inversão do ônus da prova em favor dos titulares, baseada na vulnerabilidade informacional, e a responsabilidade solidária entre agentes de tratamento, que também foram temas abordados com maior frequência.

O resultado do estudo reflete uma consolidação da cultura de proteção de dados pessoais no Brasil que, nos processos judiciais, deixou de ser aplicada de forma incidental e passou a fazer parte do debate central das decisões.

Ministério da Justiça implementa o uso de inteligência artificial em investigações criminais

Em um mundo cada vez mais digital, a recente portaria do Ministério da Justiça, publicada em 30 de junho de 2025, acompanhou a evolução tecnológica ao autorizar o uso de inteligência artificial (IA) com reconhecimento facial à distância em investigações criminais.

A referida Portaria estabeleceu diretrizes claras que permitem o uso de IA em situações específicas, como investigações criminais, previamente autorizadas pela Justiça, que carecem de outros meios de prova; buscas por pessoas desaparecidas ou que foram vítimas de crime; e recaptura de detentos foragidos. Além disso, a tecnologia pode ser aplicada em flagrantes de crimes com penas superiores a dois anos, desde que com a imediata comunicação à autoridade judicial.

É importante destacar que, para outros casos, o uso da IA deve ser justificado e analisado quanto aos potenciais impactos negativos, garantindo que a implementação respeite os princípios legais e os direitos fundamentais.

O principal objetivo da Portaria é padronizar procedimentos para o uso de tecnologia pelos órgãos de segurança pública, federais e estaduais, com o intuído de assegurar a proteção de dados sensíveis e prevenir acessos não autorizados.

Mais ainda, possibilita a identificação de dispositivos móveis em estabelecimentos prisionais, permitindo o bloqueio de sinais e a apreensão de aparelhos, além da coleta de dados de dispositivos eletrônicos apreendidos, com supervisão do Judiciário.

Essa nova regulamentação demonstra o compromisso do órgão do governo federal brasileiro em acompanhar as inovações tecnológicas, visando resultados eficazes através do uso da IA com o devido cuidado à proteção de dados pessoais.

STJ reconhece responsabilidade objetiva de plataforma de criptomoedas por falha em segurança, mesmo com autenticação em dois fatores

Em decisão unânime, a Quarta Turma do Superior Tribunal de Justiça (STJ) reafirmou a responsabilidade objetiva de plataformas de investimento em criptomoedas por fraudes ocorridas em seus sistemas, mesmo quando há uso de autenticação em dois fatores. O julgamento do Recurso Especial nº 2.104.122/MG, relatado pela Ministra Maria Isabel Gallotti, foi concluído em 20 de maio de 2025.

O caso envolveu um investidor que teve seus bitcoins transferidos indevidamente – cerca de 3,8 bitcoins, equivalentes, na época, a aproximadamente R$ 200 mil –, apesar de a operação exigir login, senha, PIN e confirmação por e-mail. A plataforma alegou que a culpa seria exclusiva do usuário e de terceiros (hackers), tese acolhida pelo tribunal de origem.

Contudo, o STJ reformou a decisão, destacando que a corretora, por ser considerada instituição financeira — conforme o artigo 17 da Lei nº 4.595/1964 e a Súmula 479 do STJ —, responde objetivamente por fraudes decorrentes de falhas em seu ambiente digital. A Corte ressaltou que a responsabilidade só poderia ser afastada mediante prova de culpa exclusiva da vítima ou de terceiros, o que não ocorreu no caso.

A ministra relatora enfatizou que a transação fraudulenta foi concluída com múltiplas camadas de autenticação, o que evidencia falha no sistema de segurança da empresa. Assim, foi reconhecido o dever de indenizar o investidor pelos prejuízos materiais e morais.

A decisão reforça a jurisprudência do STJ sobre a proteção do consumidor em ambientes digitais e impõe maior rigor às plataformas de criptoativos quanto à segurança de suas operações.

TRT-15 afasta provas digitais para proteger privacidade de trabalhadora

O Tribunal Regional do Trabalho da 15ª região decidiu por proibir a utilização de dados de geolocalização para proteger a privacidade da trabalhadora envolvida. Essa decisão foi tomada após discordância entre as partes sobre a sentença anterior da 6ª vara do Trabalho de Campinas/SP.

A trabalhadora questionou os critérios de cálculo das horas extras, enquanto o empregador alegou que houve cerceamento de defesa, em especial, pela negativa do uso de dados de geolocalização da trabalhadora como prova.

O Tribunal destacou que o juiz tem a liberdade de indeferir diligências que considerar desnecessárias. No caso, a geolocalização foi considerada dispensável, uma vez que já havia provas suficientes nos autos. Além disso, concluiu que a requisição de dados de geolocalização poderia violar a privacidade da reclamante e retrasar o processo sem garantir a utilidade necessária.

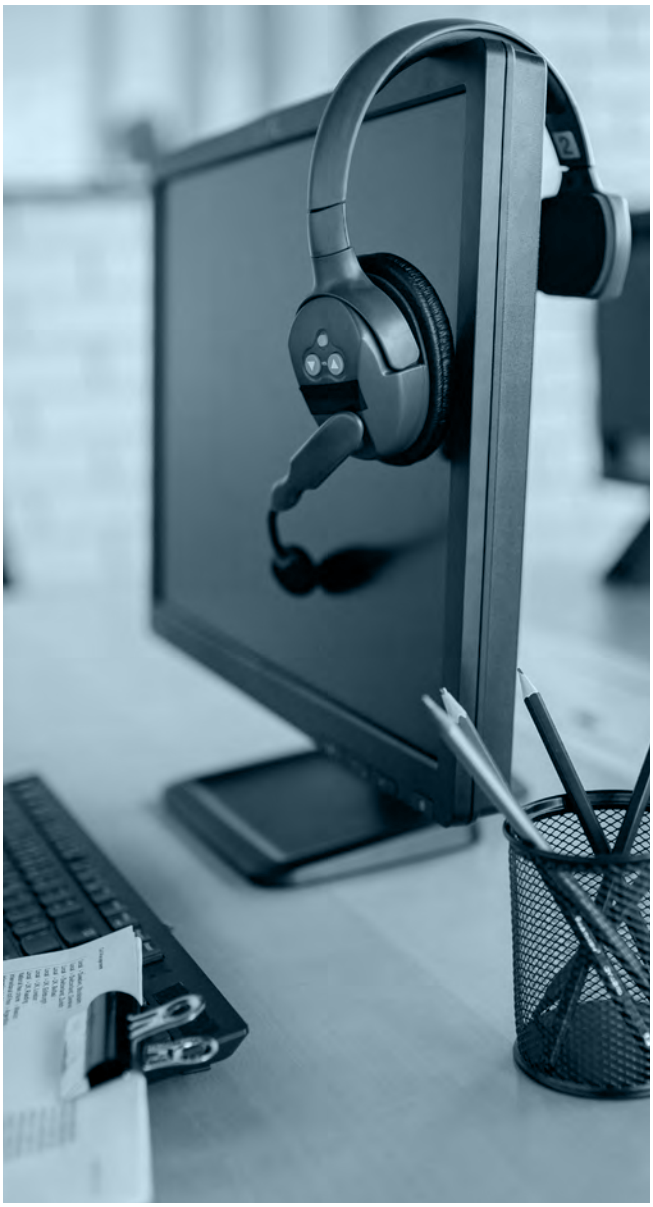
O julgamento do caso demonstrou a atenção do Tribunal aos princípios de proteção de dados, em especial os princípios da finalidade e necessidade.

Cibersegurança em foco: riscos crescentes, resposta regulatória e o papel estratégico da governança jurídica

Em um mundo cada vez mais conectado, a cibersegurança deixou de ser um tema técnico relegado aos bastidores da infraestrutura digital e passou a ocupar um espaço central nas estratégias institucionais, nas agendas regulatórias e na preocupação cotidiana de empresas, governos e cidadãos. A crescente sofisticação dos ataques cibernéticos, associada à elevada dependência de sistemas digitais para serviços críticos — como saúde, logística e finanças — impõe um cenário de atenção constante, em que falhas na proteção de dados podem gerar impactos severos e duradouros, tanto do ponto de vista operacional quanto reputacional e jurídico.

O caso recente da C&M Software ilustra com clareza esse panorama. A empresa de tecnologia, que atua como integradora entre instituições financeiras e o Banco Central, teve seus sistemas invadidos, o que resultou na exposição de milhões de registros e dados pessoais — incluindo CPFs, dados financeiros e transações bancárias. O ataque hacker, que pode ter envolvido o desvio de R$ 500 milhões, já é considerado o maior ataque cibernético da história do sistema financeiro brasileiro. O incidente teve repercussão imediata, não apenas pela quantidade de pessoas afetadas, mas pelo fato de envolver uma grande cadeia de atores financeiros, ampliando o alcance e a complexidade do vazamento.

Outro aspecto de destaque neste caso é a suspeita de que o ataque possa ter sido possibilitado por um funcionário da C&M Software, que teria fornecido dados internos e credenciais da empresa ao grupo responsável pelo ataque em troca de retorno financeiro.



Diante desse cenário, a Autoridade Nacional de Proteção de Dados (ANPD) vem fortalecendo sua estrutura institucional e atuação estratégica para lidar com os desafios internos de segurança da informação. Em maio de 2025, a autoridade anunciou a criação do Comitê de Segurança da Informação (CSIN) e da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (EPTIC). O CSIN atuará no planejamento e na formulação de diretrizes internas de segurança cibernética, com foco na proteção dos próprios ativos informacionais da ANPD, enquanto a EPTIC terá papel mais técnico e operacional, assumindo a linha de frente na contenção e análise de incidentes, incluindo tentativas de invasão e falhas de integridade em bases de dados sob gestão pública.

Essas iniciativas integram uma visão mais ampla da ANPD, refletida em sua agenda regulatória para o biênio 2025–2026. A agenda aborda diversos temas críticos, incluindo a regulação do Art. 46 da Lei Geral de Proteção de Dados (LGPD), que dispõe sobre a obrigatoriedade da adoção de medidas de segurança, técnicas e administrativas pelos agentes de tratamento, aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. O § 1º do referido artigo permite à ANPD dispor sobre padrões técnicos mínimos relacionados a essas medidas — um passo que se torna cada vez mais urgente diante da multiplicação dos incidentes.

Em 2021, a autoridade publicou um guia de segurança da informação para agentes de tratamento de pequeno porte relacionado ao tema, o qual inclui um checklist de medidas de segurança e, em abril de 2024, foi publicado o Regulamento de Comunicação de Incidente de Segurança, que estabelece os procedimentos para comunicação de incidentes que possam acarretar risco ou dano relevante aos titulares. No entanto, ainda há espaço para novas instruções sobre esse assunto, sendo possível esperar futuras orientações da ANPD quanto a este tema.

A inclusão da cibersegurança como eixo estruturante na atuação da ANPD também é coerente com o crescente volume de notificações de incidentes de segurança. Somente no primeiro semestre de 2025, foram recebidos 217 comunicados de violação, envolvendo o setor público e o privado. Dentre esses, destacam-se ataques relacionados ao roubo de credenciais/engenharia social e sequestro de dados (ransomware).

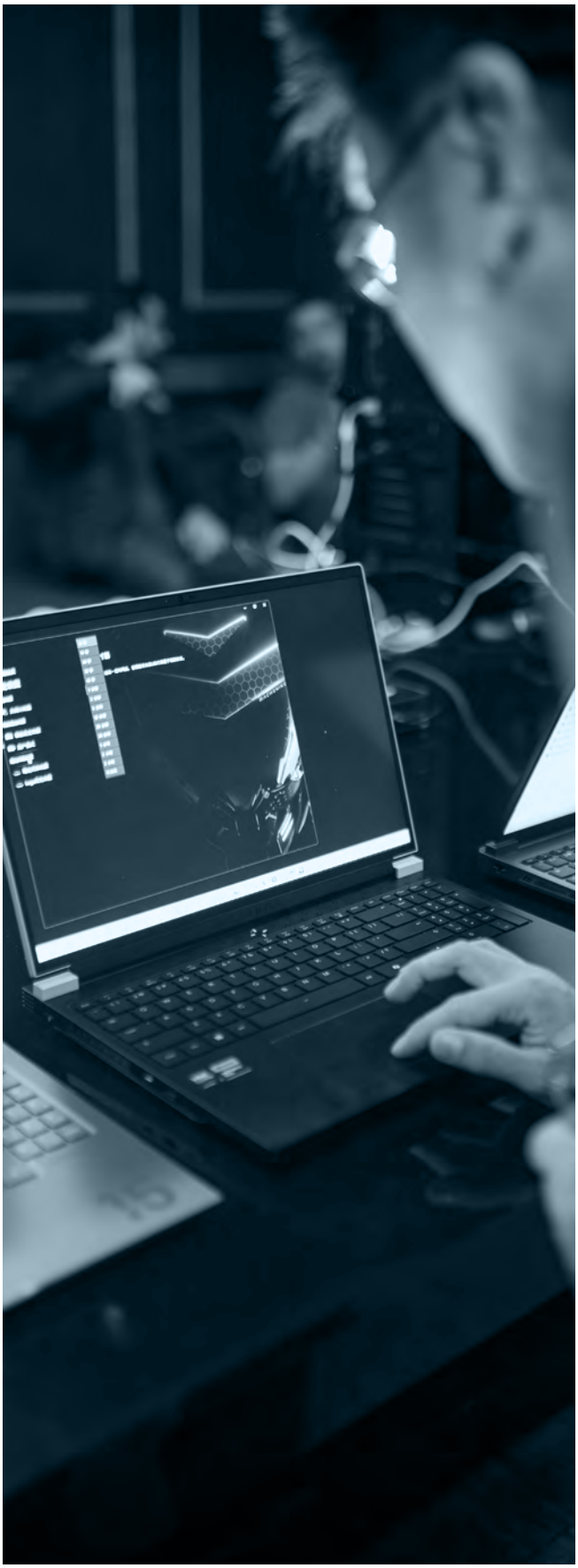
Para além das iniciativas públicas mencionadas, o setor privado desempenha papel decisivo no que tange à cibersegurança de empresas e organizações do setor. A cibersegurança não deve ser vista como um custo, mas como um ativo estratégico, diretamente vinculado à reputação institucional, à confiança dos usuários e à própria viabilidade jurídica de suas operações. A exigência de medidas de segurança prevista na LGPD não deve se limitar à implantação de firewalls ou antivírus, devendo abranger políticas internas de governança,

planos de resposta a incidentes, treinamentos recorrentes, auditorias independentes e uma cultura de segurança que permeie todos os níveis da organização.

No entanto, o cenário ideal de cibersegurança ainda não é uma realidade para a maior parte do setor privado. Por exemplo, um levantamento da Federação das Indústrias do Estado de São Paulo (Fiesp) revelou que, no estado, apenas 44,2% das empresas respondentes possuem uma estrutura organizacional de segurança cibernética ou da informação. Além disso, 52,4% dessas empresas não tratam a cibersegurança como prioridade, apesar de enxergarem como algo necessário. Dentre os desafios enfrentados pelas empresas na implementação da LGPD, o treinamento e a conscientização foram indicados como os principais.

Em tempos de transformação digital acelerada, sofisticação de ataques e de regulação cada vez mais atenta, o papel do jurídico vai muito além do contencioso pós-incidente. Casos recentes não deixam dúvidas: é essencial estabelecer um ecossistema de cibersegurança sólido e bem estruturado, além de estimular o alinhamento de todos os funcionários da empresa a essa cultura.

Nesse contexto, o fortalecimento da cultura de proteção de dados e da cibersegurança deve ser prioridade transversal. O momento exige do setor público, do setor privado e da sociedade civil um compromisso ativo com a construção de ambientes digitais mais seguros, transparentes e responsáveis.



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