TozziniFreire.
ADVOGADOS

Boletim
Cybernews.

4ª 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 Cybernews, destacamos o uso de inteligência artificial (IA) como causa de aumento de pena na violência de gênero e as principais notícias sobre proteção de dados no mês de maio de 2025.

O Supremo Tribunal Federal (STF) penaliza advogado por petição com conteúdo gerado por IA e oficia o Conselho Federal da Ordem dos Advogados do Brasil (OAB) e OAB da Bahia para que adote as providências cabíveis. A decisão constatou que no caso houve o uso indiscriminado de IA sem a adequada revisão humana e com a apresentação de informações falsas.

Além disso, o governo também criou grupo de trabalho para elaboração do chamado Plano Nacional de Cibersegurança, cujo objetivo é interagir com órgãos da administração pública federal para identificar ações, em andamento ou previstas, que sejam compatíveis com o estipulado pela Política Nacional de Cibersegurança (PNCiber) e pela Estratégia Nacional de Segurança Cibernética (Ciber).

A 3ª Turma do Superior Tribunal de Justiça (STJ) decidiu que vítimas de golpistas que tenham seus dados sigilosos bancários acessados podem reivindicar indenização por dano moral presumido. A decisão foi baseada em um caso em que um indivíduo pagou um boleto falso com informações confidenciais, como valor e número de parcelas, que apenas o banco poderia conhecer.

Por fim, o 1º Juizado Especial Cível de Planaltina, no Distrito Federal, condenou um personal trainer a pagar indenização por danos morais a um aluno, pela utilização não autorizada de sua imagem em um vídeo publicado em sua conta, no Instagram. A decisão se fundamentou na Lei Geral de Proteção de Dados (LGPD), para concluir que o tratamento dos dados do aluno, como a divulgação de sua imagem, deveria ter como base o seu consentimento "livre, informado e inequívoco".

NOTÍCIAS GERAIS

O uso de IA como causa de aumento de pena na violência de gênero

A promulgação da Lei nº 15.123/2025 representa um avanço significativo no combate à violência psicológica contra as mulheres, especialmente no ambiente digital, no qual os crimes de gênero têm crescido exponencialmente. A lei estabelece uma causa de aumento de pena para o crime de violência psicológica contra as mulheres, quando "cometido mediante uso de inteligência artificial ou de qualquer outro recurso tecnológico que altere imagem ou som da vítima", de acordo com novo parágrafo único do artigo 147-B do Código Penal.

Violência psicológica e a nova lei

A vulnerabilidade de determinados grupos sociais, especialmente mulheres e jovens, torna-se evidente e crescente no espaço digital. A violência de gênero nesse meio inclui práticas como *revenge porn*, disseminação de *fake news*, criação de perfis falsos nas redes sociais, *deep fakes* e manipulação de imagens. Esse problema social é impactado pelo novo texto em caráter punitivo e preventivo, uma vez que reforça a necessidade de mudanças da sociedade em relação a tais condutas.

O artigo 147-B do Código Penal define que a violência psicológica se dá por meio de ações que causam danos emocionais às mulheres e que prejudicam e perturbam seu pleno desenvolvimento ou que visam a degradar ou a controlar suas ações, comportamentos, crenças e decisões, mediante ameaça, constrangimento, humilhação, manipulação, isolamento, chantagem, ridicularização, limitação do direito de ir e vir ou qualquer outro meio que cause prejuízo à saúde psicológica e autodeterminação. Com a nova lei, nas situações em que o tal crime for cometido através do uso de IA ou outro recurso tecnológico que modifique imagem ou som da vítima, a pena é aumentada pela metade.

Violência digital de gênero e avanços legislativos

Dados da SaferNet revelaram que o português é o segundo idioma com mais denúncias de violência e discriminação contra mulheres nas plataformas online. Essa estatística ressalta a urgência de uma resposta legislativa adequada a esse grave problema social. A

introdução da causa de aumento de pena pela Lei nº 15.123/2025 é um avanço e exemplo disso.

A última década teve um aumento considerável dos crimes praticados no ambiente digital, o que tem sido objeto de propostas legislativas, com o intuito de coibir crimes praticados nesse espaço. Do mesmo modo, o Código Penal já contém dispositivos que criminalizam a invasão de dispositivos eletrônicos, a divulgação não autorizada de imagens íntimas e até a ciberviolência, como a Lei nº 12.737/2012 – conhecida como "Lei Carolina Dieckmann" -, que criminaliza a invasão de dispositivo informático mediante violação, com o fim de obter, adulterar ou destruir dados ou informações sem autorização.

A Lei nº 15.123/2025 traz o primeiro tipo penal especificamente relacionado à IA e demonstra, por um lado, a atual falta de mecanismos específicos para combate à violência de gênero nesses ambientes e, de outro, a atenção dada pelos legisladores e autoridades de diversos setores da sociedade ao tema. É esperado que sejam publicados mais Projetos de Lei (PL), guias orientativos, entre outras medidas, com intuito de estabelecer maior proteção aos direitos humanos, fomentar projetos de diversidade e inclusão, e coibir práticas discriminatórias.

De acordo com a Agenda Regulatória para o biênio 2025-2026, publicada pela Autoridade Nacional de Proteção de Dados (ANPD), a regulamentação da IA segue sendo prioridade do órgão para este e os próximos anos. A ANPD tem enfatizado a relevância de sua atuação nesse campo, principalmente considerando que a tecnologia está intrinsecamente relacionada à proteção de dados pessoais.

Ademais, o PL nº 2.338/2023, que visa regulamentar a IA no Brasil, teve seu texto aprovado pelo Senado e aguarda apreciação pela Câmara dos Deputados, o que não deve ocorrer antes de novembro deste ano. Diversos temas seguem em discussão, como classificação de riscos, direitos autorais, proteção de dados pessoais, entre outros. O PL proíbe sistemas considerados de risco excessivo, especialmente aqueles que possam comprometer a proteção de direitos fundamentais, como no combate à violência de gênero.

O texto também proíbe o uso sistemas que tenham por objetivo a produção e disseminação de material que represente abuso ou exploração sexual de crianças e adolescentes, independentemente do seu propósito, com o intuito de proteger a saúde, a segurança e a integridade física e psíquica desse grupo. De acordo com o texto da emenda que incluiu esse tema, no ano de 2023, o National Center for Missing & Exploited Children (NCMEC) dos EUA recebeu 4.700 denúncias relacionadas a esse tipo de imagem, o que demonstra a urgência do tema.

STF penaliza advogado por petição com conteúdo gerado por IA e oficia o Conselho Federal da OAB e OAB-BA para que adote as providências cabíveis

No julgamento da Reclamação 78.890, em 12 de maio de 2025, o Supremo Tribunal de Justiça (STF), por meio do ministro relator Cristiano Zanin, negou seguimento à reclamação por considerá-la manifestamente descabida.

O recurso buscava preservar a competência do STF e garantir a autoridade de sua jurisprudência vinculante – aplicação das Súmulas Vinculantes nº 6 e nº 10. Entretanto, após a análise pormenorizada do recurso, entendimento adotado pelo STF foi no sentido de que o reclamante tentou induzir o Tribunal a erro ao citar decisões inexistentes ou irrelevantes ao caso e que a Súmula Vinculante nº 6 foi citada com conteúdo falso e discrepante ao sumulado. Concluindo que o uso de informações falsas e a possível utilização de ferramenta de IA na elaboração da petição inicial, sem revisão adequada, caracterizaram má-fé processual.

Nesse cenário, restou reconhecida a má-fé e o reclamante foi condenado ao pagamento do dobro das custas iniciais e restou determinada a emissão de ofício para o Conselho Federal da OAB e para a OAB-BA para apurar possíveis violações ao Estatuto da Advocacia.

A decisão destaca a importância do rigor técnico na elaboração de petições judiciais e reforça que a reclamação constitucional não pode ser utilizada como substituto de recursos ou ações judiciais próprias. Além disso, considera temerária a forma de uso da IA ao presente caso, destacando que na minuta havia a marca d'água da ferramenta utilizada e enfatiza a responsabilidade dos advogados na utilização de ferramentas tecnológicas para evitar erros e má-fé processual.

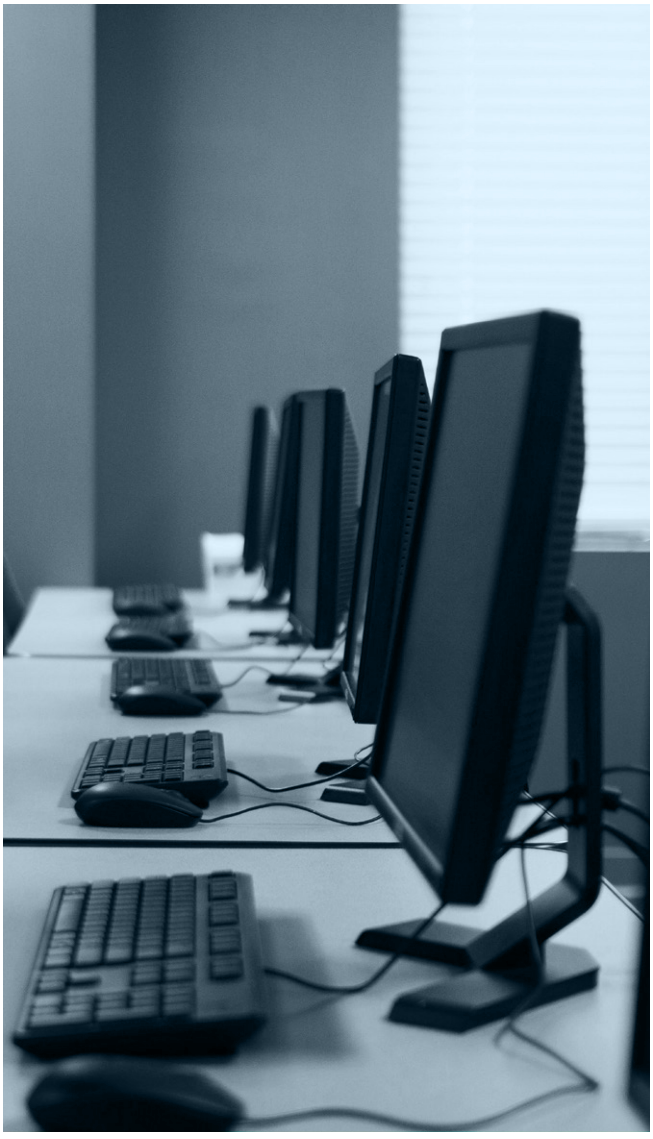
Governo cria grupo de trabalho para elaboração do Plano Nacional de Cibersegurança

O Comitê Nacional de Cibersegurança (CNCiber) vai criar um grupo de trabalho temático para elaboração do Plano Nacional de Cibersegurança (P-Ciber). O prazo de duração do grupo de trabalho temático será de até quatro meses, segundo resolução publicada em 27 de maio de 2025 no Diário Oficial da União (DOU).

Na elaboração do P-Ciber, o grupo de trabalho temático deve observar as seguintes orientações: interagir com órgãos da administração pública federal para identificar ações em andamento ou previstas, que sejam compatíveis com o estipulado pela Política Nacional de Cibersegurança (PNCiber) e pela Estratégia Nacional de Segurança Cibernética (Ciber); e agrupar as ações propostas em dois grupos, ações de curto prazo (triênio 2025-2027) e ações de médio prazo (triênio 2028-2031).

O grupo de trabalho temático, que será coordenado pelo Gabinete de Segurança Institucional da Presidência da República, contará com representantes do governo, setor empresarial e sociedade civil. Ao final das suas atividades, o coordenador do grupo de trabalho temático assinará e encaminhará relatório final à deliberação do CNCiber.

O conselho ainda publicou resoluções para criação de outros grupos de trabalho como para elaboração de guia para a criação e operação de Centros de Análise e Compartilhamento de Informações (Information Sharing and Analysis Centers); para elaboração de Guia de Requisitos Mínimos de Cibersegurança para provedores e operadores de Serviços Essenciais e de Infraestruturas Críticas (SEICs); e para identificação ou elaboração de materiais educativos de cibersegurança e estratégias de difusão desses materiais.



Acesso de golpistas a dados sigilosos de banco gera dano moral presumido, diz STJ

Em julgamento do Recurso Especial (REsp) nº 2.187.854, a 3ª Turma do Superior Tribunal de Justiça (STJ) decidiu que vítimas de golpistas que tenham seus dados sigilosos bancários acessados fazem jus à indenização por dano moral presumido.

O caso analisado envolveu uma vítima que pagou um boleto falso, sem suspeitar do golpe, uma vez que os criminosos apresentaram informações cuja guarda seria de responsabilidade do banco, que ela não havia fornecido.

O Tribunal de Justiça de São Paulo (TJSP) havia condenado o banco a ressarcir os prejuízos enfrentados, mas afastou a concessão de danos morais sob o argumento de que a correntista deveria comprová-los, como a negativação de seu nome ou a apreensão do veículo. Contudo, no STJ, embora a jurisprudência da Corte entenda que a fraude bancária, por si só, não configura dano moral, determinou-se que a presença de danos morais se aplica em casos que envolvem o vazamento de dados pessoais sigilosos.

Segundo o entendimento do acórdão, '*a configuração do dano moral decorre do evidente sentimento de insegurança experimentado pela parte ao perceber que seus dados foram disponibilizados indevidamente para terceiros, favorecendo a prática de atos ilícitos ou contratações fraudulentas por eventuais terceiros de má-fé*'.

A ministra Nancy Andrighi, relatora do recurso, concluiu que a necessidade de comprovação de efetivo prejuízo seria dispensável para se aferir o dano moral, uma vez que pode ser presumido já que houve acesso a dados sigilosos da vítima.

Personal trainer é condenado por usar imagem de aluno no Instagram

O 1º Juizado Especial Cível de Planaltina/DF condenou um personal trainer a pagar R$ 600,00 em indenização por dano moral a um aluno, devido à utilização indevida de sua imagem em vídeo em sua conta no Instagram. A imagem foi divulgada sem o consentimento, mesmo que o aluno aparecesse apenas por três segundos.

Durante o processo, o aluno relatou sua surpresa e constrangimento com a postagem. O personal trainer alegou ter obtido um consentimento genérico por meio de um contrato com a academia, porém a juíza destacou que tal acordo não contemplava o uso da imagem para o treinador específico.

A magistrada ressaltou que a Constituição assegura a inviolabilidade da imagem e que o Código Civil exige consentimento expresso para veiculação pública. Salientou, ainda, que a Lei Geral de Proteção de Dados (LGPD) impõe consentimento "livre, informado e inequívoco" para tratamento de dados pessoais. A magistrada considerou a utilização da imagem para promoção pessoal do réu como uma ação ilícita, reconhecendo o dano moral e estabelecendo a indenização com um valor que respeita a gravidade da ofensa sem gerar enriquecimento indevido para o aluno.

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