TozziniFreire.
ADVOGADOS

Boletim Cybernews.

6ª Edição | 2024

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 que permearam o cenário digital e de proteção de dados no mês de maio de 2024.

Mais de 1.700 pessoas foram presas no Brasil utilizando reconhecimento facial, mesmo sem regulamentação específica. A Bahia lidera com 1.547 prisões, seguida por Rio de Janeiro e São Paulo, que também relataram detenções. Vários estados estão implementando a tecnologia, mas surgem preocupações quanto à precisão e justiça.

Enquanto isso, o Banco Central informou sobre vazamentos de dados de chaves PIX envolvendo Iugu e Pagcerto, afetando 22.046 chaves. Os dados expostos são de natureza cadastral e medidas de apuração estão em andamento.

A Ticketmaster confirmou o vazamento de dados de 560 milhões de clientes. A Live Nation investiga o incidente, enquanto o Procon-SP notificou a empresa para esclarecer o impacto aos clientes brasileiros. A Autoridade Nacional de Proteção de Dados (ANPD) poderá exigir explicações adicionais. No âmbito do Poder Judiciário, o Tribunal Superior do Trabalho (TST) autorizou o Banco Santander a usar prova de geolocalização para comprovar a jornada de um bancário. A medida foi considerada adequada e proporcional, sem violar a privacidade.

NOTÍCIAS GERAIS

Sem regulamentação, estados brasileiros usam reconhecimento facial para prender pessoas

Um levantamento da revista eletrônica Consultor Jurídico revelou que mais de 1.700 pessoas foram presas no Brasil com o uso de reconhecimento facial, mesmo sem regulamentação específica. A Bahia lidera, com 1.547 prisões desde 2019, seguida por outros estados que utilizam a tecnologia, mas não divulgam números detalhados.

São Paulo relatou 52 prisões de procurados pela Justiça e outras detenções relacionadas a medidas judiciais e uso de documentos falsos. No Rio de Janeiro, mais de 130 pessoas foram detidas desde a implementação na última virada de ano. Roraima deteve 15 pessoas em eventos como festas juninas e feiras agropecuárias, enquanto Sergipe realizou oito detenções, apesar de dois casos de prisões equivocadas.

Outros estados, como Acre, Maranhão e Pará, admitiram o uso do reconhecimento facial, mas não especificaram o número de prisões. Em Minas Gerais, testes no Carnaval foram bem avaliados, mas sem detenções.

Vários estados, incluindo Tocantins, Espírito Santo, Mato Grosso e Goiás, estão em processo de implementação da tecnologia. Entretanto, Santa Catarina, Paraná, Mato Grosso do Sul, Piauí, Rio Grande do Norte e o Distrito Federal não utilizam o reconhecimento facial. Paraíba, Pernambuco, Amazonas e Amapá não responderam às perguntas.

O Rio Grande do Sul não forneceu informações devido à tragédia ambiental causada por mudanças climáticas. A falta de dados sobre erros tecnológicos e impacto em pessoas pretas e pardas levanta preocupações sobre a precisão e justiça do uso da biometria.

Banco Central informa vazamento de dados de chaves PIX

O Banco Central divulgou uma nota informando sobre incidentes de segurança que resultaram no vazamento de dados pessoais vinculados a chaves PIX, sob responsabilidade das instituições de pagamento Iugu e Pagcerto. Os incidentes ocorreram devido a falhas pontuais nos sistemas dessas empresas, afetando 19.849 chaves da Iugu e 2.197 da Pagcerto.

Além disso, o Banco Central esclareceu que os dados expostos são de natureza cadastral e não incluem informações sensíveis como senhas, movimentações financeiras ou saldos de contas. As pessoas afetadas serão notificadas exclusivamente por meio do aplicativo ou internet banking de suas instituições de relacionamento, sem o uso de aplicativos de mensagens, chamadas telefônicas, SMS ou e-mails.

As ações necessárias para uma apuração detalhada já foram iniciadas e medidas sancionadoras serão aplicadas conforme a regulação vigente, segundo o Banco Central. Apesar do baixo impacto potencial para os usuários, a autoridade monetária optou por informar o público em respeito ao seu compromisso com a transparência.

Ticketmaster confirma vazamento de dados de 560 milhões de clientes

A Ticketmaster confirmou o vazamento de dados que pode ter exposto 560 milhões de clientes. A Live Nation, que subsidia a Ticketmaster, informou à SEC (Comissão de Valores Mobiliários dos EUA) que iniciou uma investigação após detectar "atividade não autorizada" em um banco de dados em nuvem de terceiros.

Em 28 de maio, o grupo hacker ShinyHunters assumiu a responsabilidade pelo ataque no fórum BreachForums, oferecendo 1,3 terabyte de dados por US$ 500 milhões. Foram vazados nomes, endereços, telefones e informações de cartões de crédito. O FBI apreendeu o domínio do fórum, conhecido por ser um dos maiores da dark web.

O Procon-SP notificou a empresa para que esclareça se clientes brasileiros foram afetados e quantos podem ter sido atingidos. A Ticketmaster deve esclarecer também como os dados são armazenados e quais medidas serão adotadas.

A Autoridade Nacional de Proteção de Dados (ANPD) informou que ainda não recebeu comunicado formal da Ticketmaster, mas poderá exigir esclarecimentos caso identifique riscos ou danos relevantes às pessoas afetadas.

PODER JUDICIÁRIO

TST autoriza o uso de geolocalização como prova de jornada de trabalho

Por maioria de votos, a Subseção II Especializada em Dissídios Individuais (SDI-2) do Tribunal Superior do Trabalho (TST) derrubou uma liminar que impedia o Banco Santander de usar prova digital de geolocalização para comprovar a jornada de um bancário de Estância Velha, no Rio Grande do Sul (RS). O colegiado considerou a prova adequada, necessária e proporcional, sem violar o sigilo garantido pela Constituição Federal.

Na ação trabalhista iniciada em 2019, o bancário, que trabalhou 33 anos no Santander, pediu pagamento de horas extras. O banco argumentou que ele ocupava cargo de gerência e não estava sujeito a controle de jornada, solicitando a geolocalização para verificar se o empregado estava nas dependências da empresa nos horários indicados.

Apesar de o bancário ter protestado, o pedido foi aceito pelo juíz da 39ª Vara do Trabalho de Estância Velha. O bancário recorreu ao Tribunal Regional do Trabalho da 4ª Região (TRT4) alegando violação de privacidade, mas o TRT4 manteve a decisão. O Santander recorreu ao TST, onde o ministro relator Amaury Rodrigues julgou a geolocalização proporcional e adequada.

O ministro ressaltou que a medida não envolve o conteúdo de comunicações, apenas a localização. Ele também mencionou que a Justiça do Trabalho possui capacitação para uso de tecnologias e que a geolocalização pode ser uma ferramenta válida para confirmar jornadas de trabalho.

Foram vencidos os ministros Aloysio Corrêa da Veiga, Dezena da Silva e a desembargadora Margareth Rodrigues Costa, que defenderam que a geolocalização deveria ser uma prova subsidiária, não principal, por considerarem a medida invasiva.

O TST informou que a produção de prova digital é respaldada por legislações brasileiras e internacionais, como a Lei Geral de Proteção de Dados Pessoais (LGPD), a Lei de Acesso à Informação e o Marco Civil da Internet.

LEGISLAÇÃO INTERNACIONAL

Novas diretrizes europeias sobre o uso e desenvolvimento de sistemas de IA generativa

Em 3 de junho, o European Data Protection Supervisor (EDPS) publicou um guia orientativo com conselhos práticos relativos à proteção de dados pessoais no uso e/ou desenvolvimento de sistemas de inteligência artificial (IA) generativa para órgãos e instituições da União Europeia (UE), de acordo com o Regulamento Europeu de Proteção de Dados (GDPR, na sigla em inglês) (acesse aqui).

Sem prejuízo das normas e diretrizes constantes do Marco Legal Europeu de Inteligência Artificial (AI Act), destacamos alguns dos principais conselhos trazidos no guia:

- **Encarregado** – o guia enfatiza a função de aconselhamento e assistência independente do Encarregado, no que se refere ao tratamento de dados pessoais por sistemas de IA generativa. O Encarregado deve entender como o sistema opera, envolver-se em decisões automatizadas e garantir transparência aos titulares de dados. Também é importante que o Encarregado participe da criação do Relatório de Impacto à Proteção de Dados (RIPD) e mantenha um inventário dos sistemas de IA generativa utilizados.

- **Relatório de Impacto à Proteção de Dados** – o documento também recomenda a elaboração de um RIPD antes de operações arriscadas, o que inclui novas tecnologias como a IA generativa. Os desenvolvedores de sistemas de IA devem consultar o Encarregado e tomar medidas para reduzir os riscos. É importante rever os riscos ao longo do ciclo de vida da IA documentando as decisões adotadas para garantir transparência e conformidade.
- **Bases legais** – sem prejuízo da aplicação de outras bases legais para atividades envolvendo IA generativa, o guia do EDPS aborda com mais detalhes duas delas: o legítimo interesse e o consentimento. O legítimo interesse pode ser utilizado para coletar dados para validar, treinar e testar o sistema de IA, observando as situações em que o teste de balanceamento é necessário. A aplicação da base legal do consentimento é delicada e deve ser feita com cautela, especialmente quando dados públicos são tratados para fins de treinamento de sistemas de IA. Caso o consentimento seja revogado, o controlador deve interromper o tratamento caso não haja outra base legal aplicável, o que pode tecnicamente impactar o sistema de IA.
- **Princípio da minimização de dados** – para garantir a privacidade dos titulares, é essencial controlar e minimizar o uso de dados pessoais em modelos de IA generativa, assegurando alta qualidade, rótulos precisos e documentação clara.
- **Princípio da precisão dos dados** – outra recomendação consiste na verificação e validação constante da estrutura e do conteúdo das bases de dados utilizadas no treinamento do sistema de IA, especialmente se adquiridas de terceiros, para garantir a precisão dos dados. Monitorar resultados, adotar cláusulas contratuais para garantir a precisão dos dados e realizar testes são medidas importantes para evitar distorções nos sistemas de IA.
- **Transparência na IA** – desenvolvedores dos sistemas de IA devem fornecer informações sobre as diversas etapas de seu processo de desenvolvimento, bem como da origem dos dados, entre outras informações que forem pertinentes. Quando houver interação com humanos, o usuário deve ser informado que está interagindo com um sistema de IA.
- **Tomada de decisões automatizadas** – nos casos em que o sistema de IA generativa for utilizado para tomada de decisões automatizadas, o usuário deve ser informado sobre a lógica do sistema, funcionamento do algoritmo e bases de dados utilizados, garantindo a revisão humana.
- **Transferência internacional de dados** – quando o uso do sistema de IA envolver transferência internacional de dados, será necessário seguir as bases legais do GDPR para garantir sua conformidade.

As orientações emitidas pelo EDPS, em conformidade com o GDPR, oferecem diretrizes valiosas não apenas para empresas e instituições europeias, mas também servem de norte para empresas brasileiras que buscam antecipar e mitigar riscos associados aos sistemas de IA generativa. Ao seguir as recomendações do guia, as instituições têm a oportunidade de enfrentar os desafios e identificar as vantagens decorrentes do uso responsável e transparente de tecnologias pautadas em sistemas de IA. Esse alinhamento com as melhores práticas estabelecidas contribui para uma abordagem ética e eficaz na implementação de tecnologias que utilizam sistemas de IA alinhando-se aos princípios globais de proteção de dados.

Olhando para a realidade brasileira, o Marco Legal da Inteligência Artificial ainda está sendo discutido no Congresso Nacional. Era aguardada uma definição sobre o assunto no dia 18 de junho de 2024, mas a votação foi adiada devido à apresentação de uma nova versão do Projeto de Lei (PL) pela Comissão Temporária Interna sobre Inteligência Artificial no Brasil. Dentre as alterações propostas, destaca-se a definição da Autoridade Nacional de Proteção de Dados (ANPD) como entidade responsável por coordenar o Sistema Nacional de Regulação e Governança de Inteligência Artificial (SIA). Como resultado da apresentação dessa nova redação, a votação do Marco Legal da IA foi postergada e ocorrerá após a realização de cinco audiências públicas sobre o tema na comissão.

Enquanto aguardamos uma definição sobre o PL que visa regular a utilização de sistemas de IA no Brasil, merece destaque o papel que a ANPD vem tendo frente a esse tema. A autoridade já publicou uma série de documentos analisando o atual PL, apresentou contribuições ao texto substitutivo proposto pelo senador-relator do PL e, ainda, incluiu em sua agenda regulatória para o biênio 2023-2024 a previsão da edição de ações envolvendo a temática.

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

Colaboraram para este boletim:

Beatriz Guthmann Spalding
Carolina Vargas Pêgas Bonfante
Caroline Cristina Malheiros
Igor Baden Powell
Isabella de Freitas Moraes Sampaio Pereira
Julia Parizotto Menzel
Julie Lissa Kagawa
Luciana Pinto de Azevedo
Maria Eugênia Geve de Moraes Lacerda
Mariana Costa Alvarenga
Miguel Lima Carneiro
Steffani da Silva Nepomuceno
Tatiane Robles Martins
Valentina Garcia de Victor