TozziniFreire.
ADVOGADOS

Boletim Cybernews.

4ª 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

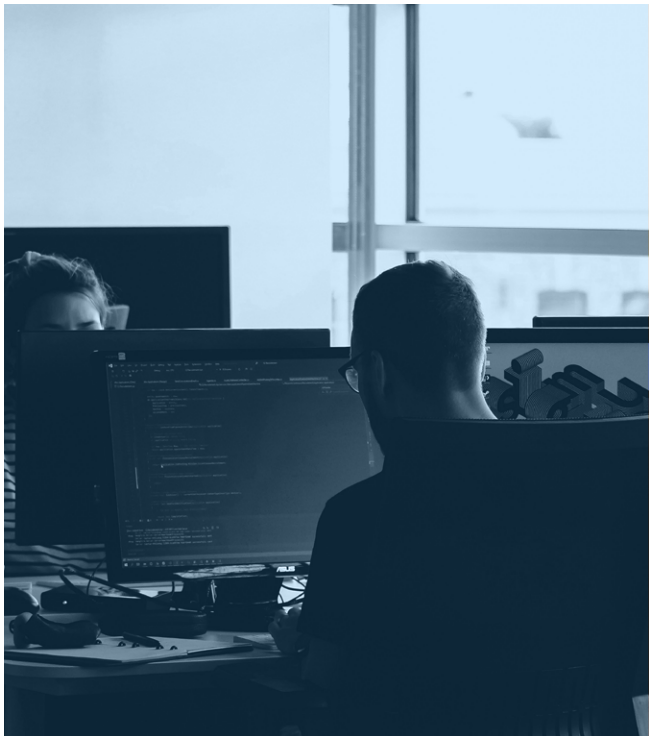
Nesta edição do Boletim CyberNews, destacamos as principais notícias que permearam o cenário digital e de proteção de dados no mês de abril de 2024.

No boletim passado, discutimos o fortalecimento do compromisso pela aplicação da Lei Geral de Proteção de Dados (LGPD) na atuação do Ministério Público do Trabalho e Emprego em relação ao seu posicionamento para a manutenção do Relatório de Igualdade Salarial, bem como na atuação da Prefeitura de São Paulo ao assumir Presidência do Fórum de Proteção de Dados Municipais e do Ministério Público nas investigações sobre o uso do CPF para oferecer descontos em farmácias.

Já neste mês, apontamos que os desafios continuam tendo em vista que as empresas enfrentam pressão para cumprir prazo de divulgação de relatórios de igualdade salarial. Em decisão recente, o Tribunal Regional Federal (TRF) da 6ª Região suspendeu os efeitos da liminar que desobrigou empresas com 100 ou mais funcionários a divulgar relatórios de transparência salarial.

Em outra frente, houve o avanço da implementação do '*open health*' no Brasil e a Federação das Indústrias do Estado de São Paulo (Fiesp) promoveu evento para discutir as maneiras mais adequadas de responder a um incidente cibernético. Ainda, a Polícia Federal prendeu o suspeito do maior vazamento de dados do Brasil – ocorrido no ano de 2021.

Também é destaque a atuação do legislativo, pelo do Conselho Nacional dos Direitos da Criança e do Adolescente (Conanda), na aprovação da Resolução Conanda nº 245/2024, que dispõe sobre os direitos das crianças e adolescentes em ambiente digital, bem como na discussão do Projeto de Lei Complementar (PLP) nº 234/2023, que pretende instituir a Lei Geral de Empoderamento de Dados (LGED), a qual disporá sobre o ecossistema brasileiro de monetização de dados no Brasil.



LEGISLATIVO

Aprovada a Resolução nº 245/2024 do Conanda, sobre direitos das crianças e adolescentes em ambiente digital

No início de abril de 2024 foi aprovada a Resolução Conanda nº 245/2024, que dispõe sobre os direitos das crianças e adolescentes em ambiente digital.

Em resumo, a Resolução destaca a importância das tecnologias digitais no cenário contemporâneo, sublinhando seu papel tanto na promoção quanto no risco aos direitos de crianças e adolescentes. O termo "ambiente digital" é aplicado a uma ampla gama de tecnologias de informação e comunicação, incluindo a internet, dispositivos conectados, realidade virtual e aumentada, inteligência artificial, robótica, e outros sistemas avançados, alinhados com as diretrizes do Comentário Geral nº 25 de 2021 do Comitê dos Direitos da Criança da Organização das Nações Unidas (ONU).

A resolução, dividida em seis capítulos, discute medidas essenciais para proteger os interesses das crianças e adolescentes online, com o objetivo de garantir seu bem-estar digital. Ela também aborda o direito à liberdade de expressão, privacidade e proteção de dados pessoais.

Com base no artigo 227 da Constituição Federal, o Conanda enfatiza a responsabilidade compartilhada entre diversos setores da sociedade para proporcionar uma experiência online segura e enriquecedora para o público jovem. Isso inclui o comprometimento do governo e das empresas provedoras de produtos e serviços digitais em combater a exclusão digital e a discriminação, além de promover a conscientização sobre as influências, tanto positivas quanto negativas, do mundo digital nas crianças e adolescentes.

Como parte dessa iniciativa, também faz parte da proposta do documento o desenvolvimento, em até 90 dias a partir da sua publicação, da "Política Nacional de Proteção dos Direitos da Criança e do Adolescente no Ambiente Digital" pela Secretaria Nacional dos Direitos da Criança e do Adolescente (SNDCA) e pelo próprio Conanda.

NOTÍCIAS GERAIS

TozziniFreire Advogados sedia evento “PrivacyRules 2024 Latin American Conference”

No dia 11 de abril de 2024, TozziniFreire sediou o evento “PrivacyRules 2024 Latin American Conference”, organizado em conjunto com *PrivacyRules* – aliança global de escritórios de Privacidade e Proteção de Dados –. Os participantes tiveram a oportunidade de conversar com autoridades, advogados, encarregados e diretores jurídicos de empresas ao redor do mundo sobre proteção de dados em uma perspectiva globalizada.

O evento proporcionou discussões muito produtivas cobrindo diversas jurisdições. Por esse motivo, compartilhamos com vocês os principais tópicos discutidos:

I. COMO LIDAR COM INCIDENTES DE SEGURANÇA DA INFORMAÇÃO QUE AFETAM MÚLTIPLAS JURISDIÇÕES

Dentre as diversas questões sobre qual postura as empresas devem tomar diante de um incidente de segurança da informação com impacto internacional, Stephan Mulders, advogado do escritório holandês Van Diepen; Adriana Prado, Diretora de Comunicação Estratégica da FTI Consulting; e Ignacio Salguero, DPO LatAm da Chubb, destacaram tópicos relevantes como:

- **Colaboração entre o Encarregado e o CISO** – a colaboração entre o Encarregado (DPO) e o Diretor de Segurança da Infor-

mação *(Chief Information Security Officer,* CISO) da empresa é essencial para um gerenciamento eficaz do incidente de segurança sob múltiplas perspectivas, com alinhamento de prioridades legais, técnicas e de relações públicas com stakeholders.

- **Indicação de um PMO para alinhar as prioridades** – como um incidente de segurança requer a análise e solução conjunta de diversas áreas da empresa, deve haver um *Project Management Office* (PMO) para ajudar a entender os riscos envolvidos e alinhar as prioridades legais, técnicas e de comunicação.
- **Comunicação de incidentes de segurança** – as empresas devem estar preparadas para comunicar a violação internamente e externamente, de modo a minimizar danos e gerenciar a percepção pública. Destacou-se que é essencial entender quais são os requisitos mínimos para realizar essa comunicação do incidente nos países dos titulares afetados e saber se há necessidade de comunicá-lo à(s) autoridade(s) competente(s), bem como conhecer os procedimentos legais e administrativos para tanto.
- **Possíveis consequências e responsabilidade da empresa** – as empresas devem conhecer as possíveis sanções aplicáveis e estar cientes das consequências reputacionais. Para minimizar danos, é importante adotar boas cláusulas contratuais relativas a eventuais incidentes de segurança, com previsão de indenização, além de realizar uma análise completa de riscos, conseguir demonstrar todas as medidas adotadas para conformidade com o Regulamento Geral sobre a Proteção de Dados (General Data Protection Regulation, GDPR) e a relação de causalidade e danos envolvidos no incidente.

II. DESAFIOS DA IMPLEMENTAÇÃO DE UM PROGRAMA DE CONFORMIDADE DE EMPRESAS MULTINACIONAIS CONCILIANDO AS DIVERSAS LEIS APLICÁVEIS

Moderadas por Luiza Sato, as palestrantes Gina Fonseca, diretora jurídica da Avianca; Pamela Meneguetti, diretora jurídica e de Compliance da Nuvemshop; e María Silvana Gramaglia, vice-presidente do Conselho de Privacidade LatAm na J.P. Morgan, compartilharam suas experiências e estratégias para conciliar as normas de diferentes países, enfatizando a importância de um compromisso constante com a adequação e atualização das práticas de privacidade.

- **Desafios comuns enfrentados** – **(i)** conhecer a cultura de privacidade de cada país envolvido e entender como ocorre a aplicação de normas; **(ii)** lidar e selecionar parceiros que tenham o mesmo nível de comprometimento e maturidade quanto à proteção de dados; **(iii)** criar uma cultura de proteção de dados que se perpetue na empresa de maneira contínua para todos os colaboradores e que seja adequada a todas as jurisdições envolvidas (geralmente com orçamentos limitados para tanto).
- **Sugestões de soluções** – as palestrantes compartilharam possíveis soluções como:
  - **Obtenção do reconhecimento e compromisso corporativo, além de alocação de recursos** – necessidade de

um compromisso claro e contínuo da diretoria e administração da empresa para manter sua conformidade com leis de proteção de dados, bem como a conscientização sobre a importância de recursos voltados à área.

- **Adoção de estratégias de conformidade entre diversas jurisdições** – criação de um sistema transversal que englobe os princípios básicos de proteção de dados que sejam comuns em todas as jurisdições, como o dever de transparência, prestação de contas, respeito aos direitos fundamentais dos titulares, segurança da informação, entre outros, além da priorização de adequação às jurisdições dos mercados mais relevantes e que terão tratamento de maior volume de dados.
- **Conscientização da empresa como um todo** – conscientização de todas as áreas e departamentos da empresa de que os dados dos colaboradores, parceiros e clientes são dados importantes e valiosos, e treinamento de líderes das áreas em um nível avançado, o que facilita que as informações cheguem no Encarregado e que o tratamento de dados ocorra de forma adequada desde a sua coleta.

III. AÇÕES, EXPECTATIVAS E DESAFIOS ENFRENTADOS PELAS AUTORIDADES LATINO-AMERICANAS DE PROTEÇÃO DE DADOS

- **Autoridade de Proteção de Dados Colombiana:** Grenfieth Sierra Cadena, superintendente de Proteção de Dados da Colômbia, compartilhou o panorama normativo de proteção de dados no país e as iniciativas que estão sendo adotadas para aumentar a segurança jurídica relativa ao tema.
  - Em vista dos 10 anos de vigência da Lei de Proteção de Dados colombiana, a autoridade afirmou que há exercício positivo da lei e que existe jurisprudência consolidada sobre diversos tópicos, mas que há a necessidade de atualizar seu marco normativo de acordo com as mudanças globais de governança para garantir a reciprocidade com outras jurisdições.
  - A autoridade está sempre acompanhando as atualizações normativas globais para buscar negociações e colaborações com outros países, bem como para emitir mais guias orientativos e procedimentos para a sociedade sobre práticas adequadas relacionadas ao tratamento de dados.
  - Em suas recomendações, a autoridade colombiana afirmou que as sanções visam primordialmente a prevenção de danos à sociedade, não apenas a punição. Para evitar sanções é crucial que os agentes de tratamento sempre se apoiem nos princípios de legitimidade, consentimento, proporcionalidade e necessidade para realizar um tratamento de dados, e ponderem cuidadosamente sobre os riscos e benefícios envolvidos na operação.
  - Por fim, o judiciário colombiano está implementando iniciativas de incor-

poração de novas tecnologias em seu sistema para torná-la mais eficiente, e a autoridade incentiva o desenvolvimento de novas tecnologias, como sistemas de inteligência artificial. No entanto, essas exigem acompanhamento regulatório preventivo e um reforço de níveis de segurança para garantir a proteção de dados pessoais.

- **Autoridade de Proteção de Dados Brasileira:** Kátia Cardoso, gerente de Projetos do Conselho Diretor na Autoridade Nacional de Proteção de Dados (ANPD), compartilhou que a ANPD está avançando em negociações com a União Europeia para fortalecer a legislação de proteção de dados no Brasil. Além disso, a ANPD está realizando a análise de mais de 800 comunicados de incidentes de segurança e dos processos administrativos em curso, que incluem 4 processos de monitoramento, 17 de fiscalização e 9 sancionadores.
- No mais, ela demonstrou os trabalhos futuros e em andamento da ANPD relativos a novas regulamentações e guias orientativos, que incluem temas relevantes de **(i)** tratamento de dados de crianças e adolescentes pelo Poder Público e quais são os padrões técnicos mínimos de segurança que devem ser adotados; **(ii)** direitos dos titulares; **(iii)** relatórios de impacto à proteção de dados (RIPD); **(iv)** comunicação de incidentes de segurança; **(v)** atribuições do encarregado; **(vi)** anonimização; **(vii)** tratamentos de alto risco; e **(viii)** transferência internacional de dados.

Setores público e privado dialogam em evento na Fiesp

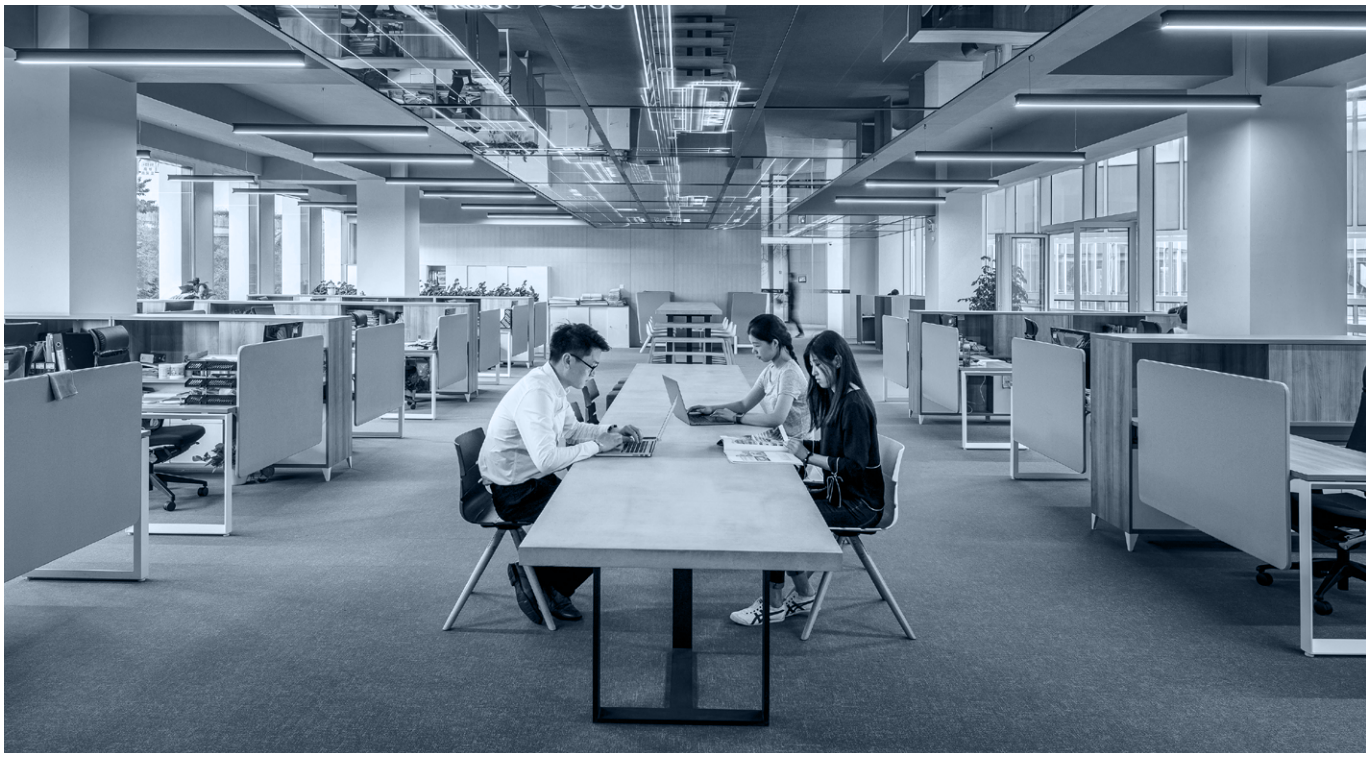
A Federação das Indústrias do Estado de São Paulo (Fiesp) promoveu evento para discutir a forma mais adequada de responder a um incidente cibernético. O seminário contou com a participação das principais autoridades administrativas em relação à proteção de dados do país e procurou trazer as experiências tanto do setor privado quanto do setor público.

Durante o evento, Waldemar Gonçalves, presidente da ANPD, anunciou que ainda esse mês será publicada resolução sobre o Comunicado de Incidente de Segurança (CIS), que irá dispor o que as organizações devem enviar à ANPD em caso de incidentes envolvendo dados de titulares. Além de esclarecer pontos essenciais para cibersegurança no país, a Resolução também trará maior segurança jurídica ao determinar com clareza as informações que precisarão ser levadas ao órgão.

Sobre o tema, Fabrício Madruga, coordenador-geral de Fiscalização da ANPD, esclareceu que o incidente de segurança não é apenas o vazamento de dados, mas também tudo aquilo que poderia prejudicar os titulares, como alterações de informações ou até indisponibilização de dados nos sistemas.

Ele trouxe que o comunicado do incidente deverá conter informações como de que forma a empresa tratou o incidente; quais os impactos aos titulares; a análise de risco; e o plano de comunicação do incidente aos titulares. Feito isso, a probabilidade da empresa ser sancionada reduz drasticamente, conforme expôs a autoridade.

Por fim, o presidente Waldemar Gonçalves explicou ainda que todas as pessoas físicas, jurídicas e organizações estão sujeitas a ataques, sendo importante não só reforçar a segurança, mas também treinar e organizar procedimentos para minimizar os danos à própria organização e a terceiros.



Empresas enfrentam pressão para cumprir prazo de divulgação de relatórios de igualdade salarial

Sob intensa disputa judicial e críticas ao governo, empresas com mais de 100 funcionários estão em uma corrida contra o tempo para preencher e publicar relatórios de transparência salarial, conforme exigido pela Lei de Igualdade Salarial. A suspensão temporária da obrigatoriedade, obtida pela FIEMG, foi recentemente revogada, desencadeando uma corrida para atender a legislação.

A presidente do TRF da 6ª Região, desembargadora federal Monica Jacqueline Sifuentes, que suspendeu os efeitos da liminar que desobrigou empresas com 100 ou mais funcionários a divulgar relatórios de transparência salarial e de critérios remuneratórios entre homens e mulheres, afirmou na decisão que, como não são divulgados nomes e dados individuais de cada empregado, não há lesão à intimidade, à privacidade ou à Lei nº 13.709, de 2018 (LGPD).

A desembargadora ainda destacou que a Lei da Igualdade Salarial "reflete o compromisso do texto constitucional em promover não apenas a igualdade formal, mas também a igualdade substancial, por meio de políticas públicas que buscam equilibrar as disparidades de gênero existentes na sociedade" (processo nº 6002520-79.2024.4.06.0000).

A FIEMG planeja recorrer da decisão, expressando preocupações sobre a exposição de dados sensíveis.

Brasil avança na implementação do "open health"

Assim como ocorreu com o open banking, o Brasil vem trabalhando pela integração de informações entre agentes do setor de saúde, com a implementação do chamado '*open health*'.

A medida visa reunir informações sobre o uso de serviços médicos e hospitalares, bem como de dados administrativos dos usuários para facilitar a contratação e portabilidade entre planos de saúde. Além disso, a expectativa é de que a integralização de dados reduza gastos no setor da saúde, possibilitando uma melhor adequação de recursos.

Desde 2022, a Agência Nacional de Saúde (ANS) conta com um Grupo de Trabalho dedicado a discussões sobre a integração de dados na saúde.

A medida está em linha com a Estratégia de Saúde Digital para o Brasil, que prevê a integração de dados até 2028.

Nesse cenário, um dos desafios à implementação do *open health* será a adequação da integração de informações à LGPD.

Pela LGPD, informações relativas ao histórico de saúde são classificadas como dados pessoais sensíveis, cujo tratamento exige consentimento expresso e específico do titular, com exceção das hipóteses previstas na própria lei.

Além disso, os dados também não poderão ser utilizados para obtenção de vantagens econômicas, salvo em condições específicas, o que também deverá ser observado no processo de integração de informações.

Outros desafios a serem enfrentados são a criação e adequação da infraestrutura tecnológica necessária à implementação do *open health*, com a criação de prontuários eletrônicos interoperáveis e a garantia de acesso adequado à internet.

Também será necessária a adoção de medidas de segurança robustas, para impedir o acesso desautorizado dos dados integrados, além da cooperação entre instituições públicas e privadas de saúde operantes no país.

Polícia Federal prende o suspeito do maior vazamento de dados do Brasil

De acordo com a Polícia Federal, o hacker investigado por vazar e comercializar informações privadas de 223 milhões de pessoas foi preso no dia 9 de abril de 2024.

O "megavazamento" de dados, ocorrido no ano de 2021, revelou informações pessoais como nome, CPF, fotografia, salário, renda, nível de escolaridade, estado civil, score de crédito e endereço de 223 milhões de brasileiros e, à época, tanto as autoridades policiais quanto as administrativas ligadas à defesa do consumidor iniciaram investigações com o propósito de identificar a fonte do incidente.

Vale relembrar também que a Secretaria Nacional do Consumidor (Senacon) e o Procon-SP chegaram a notificar a Serasa Experian, buscando o oferecimento de explicações quanto ao possível envolvimento da empresa no vazamento de dados, bem como se a empresa tem adotado medidas para melhorar a segurança da privacidade dos titulares dos dados. A empresa negou que seja a fonte dos dados e informou que colaborava com as investigações da Polícia Federal.

A ANPD também está apurando tecnicamente informações sobre o caso através do processo administrativo 00261.000050/2021-59 e coopera com os órgãos de investigação competentes para entender a origem do vazamento, a forma em que ele ocorreu, as medidas de contenção e de mitigação adotadas em um plano de contingência, bem como as possíveis consequências.

PROJETOS DE LEI

Projeto de Lei prevê a regulação de monetização de dados pessoais

O Projeto de Lei Complementar (PLP) nº 234/2023 pretende instituir a Lei Geral de Empoderamento de Dados (LGED) que disporá sobre o ecossistema brasileiro de monetização de dados, por meio da qual todas as empresas que coletam dados e informações pessoais e oferecem produtos ou serviços online deverão aderir formalmente.

O PLP nº 234/2024 tramita em regime de urgência na Câmara dos Deputados e '*tem como objetivo estabelecer um marco regulatório para a propriedade de dados e a sua monetização [...] e que pode colocar o Brasil na vanguarda em termos do tratamento do direito à privacidade de dados, ao seu tratamento e vantagens econômicas advindas do seu tratamento e compartilhamento no âmbito dos ecossistemas digitais*'.

O PLP conceitua a "monetização de dados" como a coleta, análise, agrupamento, processamento e comercialização de dados obtidos por uma instituição detentora de conta de dados ou receptora de dados mediante livre consentimento de uma pessoa física ou jurídica para a geração de receita ou benefício econômico de terceiros, por meio de plataformas eletrônicas online, aplicações de internet, marketplaces ou ecossistemas de dados.

Caso venha a ser aprovada, a proposta legislativa em questão estabelecerá um marco global pioneiro ao instituir normas para a monetização de informações tanto de cidadãos quanto de entidades empresariais, ampliando o controle dos proprietários sobre a venda desses dados. Esse assunto não foi diretamente tratado pela legislação brasileira de proteção de dados pessoais, conhecida como LGPD, que, por sua vez, não se estende a dados corporativos.

O PLP ainda não teve pareceres de Comissões da Câmara dos Deputados e atualmente aguarda distribuição para a Comissão de Ciência, Tecnologia e Inovação (CCTI).

PODER JUDICIÁRIO

TSE faz novos acordos para o combate aos deep fakes e discurso de ódio nas eleições municipais

O Centro Integrado de Enfrentamento à Desinformação e Defesa da Democracia recebeu um impulso significativo com a assinatura de acordos entre o Tribunal Superior Eleitoral (TSE), a Polícia Federal (PF) e a Advocacia-Geral da União (AGU). O objetivo da parceria é de fortalecer a luta contra as *deep fakes* e assegurar a aderência às normas estabelecidas pelo TSE em fevereiro para as eleições municipais de 2024.

Essas normas foram aprovadas em fevereiro de 2024, relatadas pela vice-presidente do TSE, ministra Carmen Lúcia. As principais instruções contra a desinformação tratam da proibição das "deep fakes", da regulamentação do uso de inteligência artificial em propagandas eleitorais e da responsabilidade de remoção de conteúdos falsos ou ofensivos por parte das plataformas de comunicação.

Inaugurado em março de 2024, o Centro tem como objetivo '*promover a cooperação entre a Justiça Eleitoral, os órgãos públicos e as big techs responsáveis pelas plataformas de redes sociais para evitar a disseminação de fake news sobre o sistema eleitoral e de discursos de ódio, sejam eles de caráter nazista, fascista, antidemocrático, racista ou homofóbico*'.

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