

BOLETIM CYBERNEWS

23ª EDIÇÃO

**Tozzini
Freire.**
ADVOGADOS



Sum

01

CONTEXTO BRASILEIRO



02

ORIENTAÇÕES GERAIS



03

AVANÇOS NORMATIVOS

anário

04

PODER JUDICIÁRIO

05

AUTORIDADES

**Tozzini
Freire.**
ADVOGADOS

Contexto Brasileiro.

Novo formulário para comunicação de incidente de segurança publicado pela ANPD

Em 23 de dezembro de 2022, a Autoridade Nacional de Proteção de Dados (ANPD) disponibilizou o novo formulário de Comunicação de Incidentes de Segurança (CIS), que deverá ser utilizado pelos controladores de dados a partir de 01 de janeiro de 2023. De acordo com a Lei Geral de Proteção de Dados (LGPD), é dever do controlador de dados comunicar incidentes de segurança que possam gerar riscos ou danos relevantes aos titulares.

Esclarecimentos adicionais, como a descrição de prováveis consequências e impactos do incidente sobre os titulares e das medidas de segurança técnicas e administrativas adotadas antes e após o incidente, são novidades na versão atualizada do formulário.

Vale dizer que um incidente de se-

gurança, conforme o entendimento da ANPD, é qualquer ocorrência confirmada que coloque em risco a confidencialidade, a integridade ou a disponibilidade dos dados pessoais dos titulares, seja intencional – como no caso de sequestro de dados ou acesso não autorizado – ou acidental – como o envio, por engano, a outro destinatário que não o pretendido.

Ainda, na avaliação de risco de um incidente com dados pessoais, deve-se observar e comunicar para fins de análise, por meio do novo formulário, o contexto da atividade de tratamento de dados; os tipos e quantidade de dados violados; os potenciais danos materiais e morais aos titulares; e as medidas de mitigação adotadas pelo controlador após o incidente.



Projeto de Lei quer incluir cadeira do CFOAB no Conselho Nacional de Proteção de Dados e da Privacidade

O Projeto de Lei (PL) nº 2.852/2022, de autoria da senadora Soraya Thronicke, propõe alterar a Lei Geral de Proteção de Dados (LGPD) para incluir uma cadeira ao representante da Ordem dos Advogados do Brasil (OAB), indicado pelo Conselho Federal da OAB (CFOAB), no Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (CNPDP), que passaria a contar com 24 representantes. A alteração seria pautada pela inclusão do possível inciso XII ao artigo 58-A da LGPD.

A justificativa do PL, conforme a parlamentar, é a importância e relevância constitucional da advocacia brasileira, que, por isso, deveria ter assento próprio no CNPDP, único colegiado público de representatividade social e multissetorial pertencente à estrutura do Estado, com notória relevância social.



Orientações Gerais.

Autoridade de Proteção de Dados do Reino Unido diz que tecnologias biométricas imaturas podem ser discriminatórias

A Autoridade de Proteção de Dados do Reino Unido (ICO) indicou preocupação com a análise incorreta dos dados biométricos e de inteligência artificial de emoções, que poderia resultar em suposições imprecisas sobre uma pessoa que, assim, levariam à sua discriminação. Na visão da ICO, as únicas aplicações biométricas viáveis serão aquelas totalmente funcionais, confiáveis e respaldadas na ciência.

Além da estratégia de repressão a organizações que tentam obter vantagens ilícitas com o uso de meios ilegais ou irresponsáveis de coleta de dados, a ICO está elaborando um guia para orientar o uso de dados biométricos, focado no aspecto pessoal do uso e coleta desse tipo de dado. As orientações têm previsão de publicação no primeiro semestre de 2023.

A ICO entende que, assim, será possível fortalecer a abordagem de “privacy by design”, entendida como privacidade desde a concepção, com o objetivo de mitigar os riscos relacionados a dados biométricos e garantir que as empresas estarão operando de maneira lícita e segura.

Autoridade Supervisora da Eslovênia decide que a segurança da propriedade pode ser considerada interesse legítimo do uso do rastreamento por GPS, desde que feito de forma adequada e necessária

Em 04 de outubro de 2022, a Autoridade Supervisora da Eslovênia decidiu que a base legal de “legítimo interesse” de proteção da propriedade pode ser aplicável para o uso de rastreamento por GPS, desde que feito de forma apropriada e necessária.

No caso em questão, após um roubo no local de trabalho em 2009, um empregador do setor privado introduziu o rastreamento por GPS de oito veículos de sua empresa, utilizados pelos funcionários para serviços de entrega. Contudo, o rastreamento era feito por um aplicativo que registrava contínua, sistemática e automaticamente a localização dos veículos e, conseqüentemente, dos funcionários identificáveis.

Após a investigação do caso, a Autoridade Supervisora da Eslovênia entendeu que o rastreamento por GPS não poderia ser utilizado de forma contínua, mas apenas quando o veículo estivesse em um local de risco e fora da supervisão do funcionário, sob pena de ser considerado uma medida intrusiva à privacidade dos funcionários.



**Avanços
Normativos.**



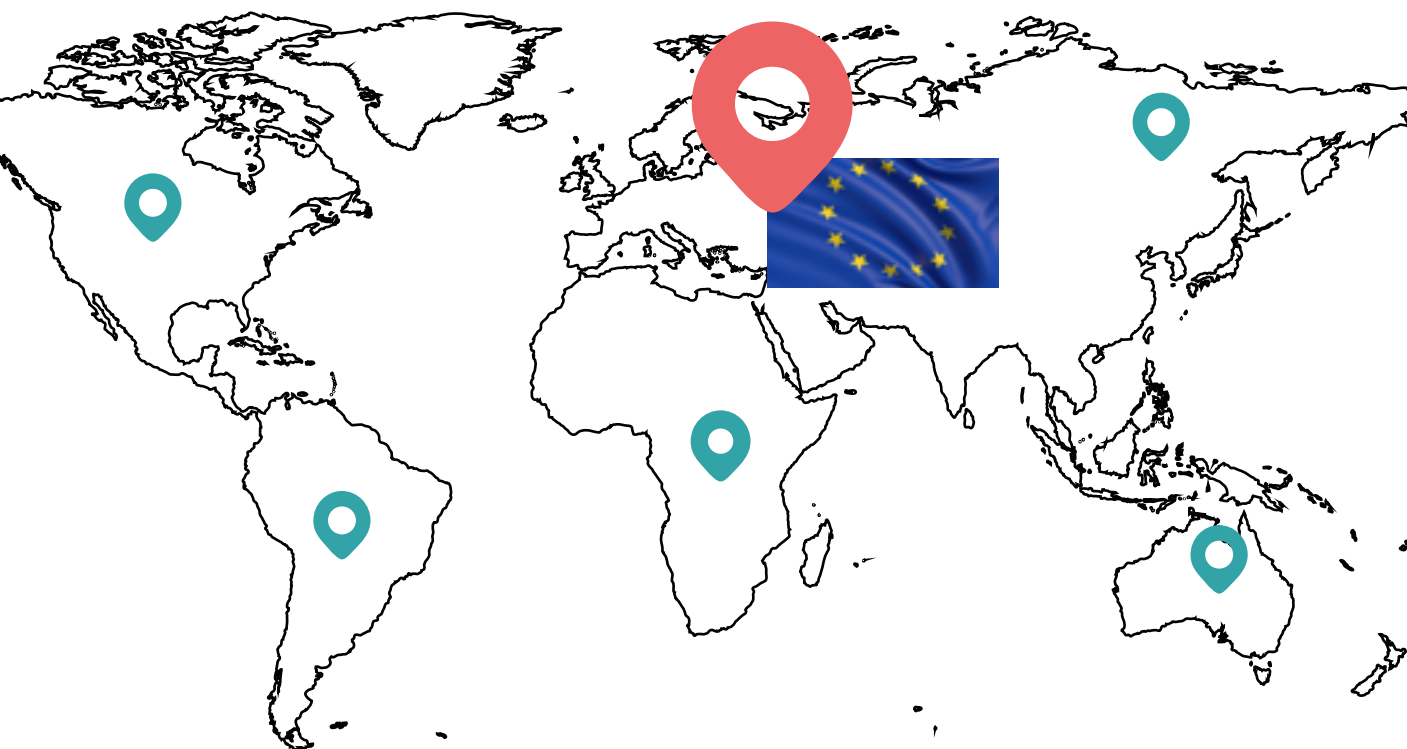
União Europeia decide fortalecer a cibersegurança e a robustez por sua extensão: Conselho da UE adota nova diretiva

O Conselho da União Europeia adotou, no final de novembro, um nível comum de cibersegurança por toda a extensão da União Europeia por meio da nova diretiva sobre cibersegurança, apelidada de “NIS2”. A expectativa do Conselho é a de que a capacidade de resposta dos entes públicos e privados aos incidentes de segurança aumente.

As principais mudanças trazidas pela NIS2 envolvem (i) a criação de quadros regulatórios para a mitigação dos riscos de cibersegurança; (ii) obrigação de reportar incidentes a todos os setores abrangidos pela diretiva, como saúde, energia, transportes e infraestrutura digital; e (iii) meios de cooperação entre as autoridades de proteção de dados dos Estados-membros.

Em relação à diretiva anterior NIS, a NIS2 passa a utilizar uma regra geral para determinar as entidades reguladas por ela, tirando essa definição do âmbito dos Estados-membros. Assim, todas as entidades de médio e grande porte dos setores abrangidos pela diretiva serão reguladas pela NIS2, excluindo-se expressamente entidades de defesa ou segurança nacional, judiciárias, parlamentares, bancos centrais, entre outras.

A NIS2 entra em vigor após 20 dias da sua publicação no Diário Oficial da UE, e os Estados-membros terão 21 meses da entrada em vigor para incorporar seus dispositivos nos ordenamentos internos.



**Poder
Judiciário.**

021

Tribunal de Justiça de São Paulo entende que Serasa está autorizada a compartilhar número telefônico de seus consumidores

Em acórdão publicado no início de novembro, a 26ª Câmara de Direito Privado do TJSP entendeu que é permitida a divulgação de dados não sensíveis para melhor proteção ao crédito.

No caso, o autor ajuizou ação requerendo que a Serasa fosse condenada a retirar de seus cadastros informações acerca dos seus dados telefônicos, bem como indenizá-lo em R\$ 10.000,00 a título de danos morais. O autor sustentou que a Serasa havia coletado e compartilhado com terceiros o seu número telefônico sem o seu consentimento, violando o seu direito à privacidade. A demanda foi julgada improcedente, de modo que a parte autora interpôs apelação.

O Tribunal agora manteve a sentença, dispondo que, por ser a ré uma

entidade cuja função é manter banco de dados relativos a consumidores, a sua conduta de comercializar o número telefônico do autor com terceiros é inerente ao seu serviço de proteção ao crédito, posto que o compartilhamento dessa informação **“facilita eventuais negociações com o consumidor e confere maior segurança aos seus eventuais credores”**.

Ainda, fundamentou que essa informação não se caracteriza como um dado pessoal sensível, nos termos do art. 5º, II, da LGPD. De acordo com o acórdão, a própria LGPD viabiliza o compartilhamento de dados pessoais visando a proteção ao crédito, conforme inteligência dos artigos 5º, II, e 7º, X, da LGPD, em conjunto com o artigo 3º, § 3º, II, da Lei do Cadastro Positivo.





Tribunal de Justiça da Paraíba afastou ordem de apresentação de código-fonte

A 3ª Câmara Cível do Tribunal de Justiça do Estado da Paraíba entendeu que a apresentação em juízo do código-fonte envolve divulgação de informação estratégica da empresa.

Para referência, um usuário ajuizou ação contra empresa de games, em razão da suspensão permanente de sua conta em um jogo eletrônico, pleiteando

(i) a apresentação do código-fonte do sistema de detecção, (ii) o reestabelecimento de sua conta e (iii) o desbloqueio do acesso ao jogo pelo seu smartphone; ou, subsidiariamente, (iv) a devolução do valor gasto dentro do jogo ou a transferência dos “bens virtuais” para uma nova conta, além do pagamento de indenização por danos morais.

Em primeiro grau, a juíza determinou à parte ré que atendesse ao pedido autoral, apresentando em juízo o código-fonte do seu sistema, com as conclusões do algoritmo utilizado por ela para suspender a conta do usuário, bem como apresentasse em juízo os dados de contato dos jogadores que teriam supostamente denunciado o autor no ambiente do jogo.

Em segundo grau, o Tribunal entendeu que a decisão não poderia prevalecer, pois envolve a divulgação de informação estratégica, que deve ser mantida em sigilo para a proteção da atividade empresarial desenvolvida pela agravante.

Pelo segundo ano consecutivo, foi publicado painel que analisa a aplicação da LGPD pelos tribunais do Brasil

O Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa (IDP) e o portal Jusbrasil – com apoio do Programa das Nações Unidas para o Desenvolvimento (PNUD) – publicaram um novo painel com a seleção das decisões judiciais mais importantes que envolvem a Lei Geral de Proteção de Dados (LGPD) pelo segundo ano consecutivo.

A pesquisa pautou-se em um sistema de inteligência artificial que possibilitou a análise de 1.789 documentos da justiça brasileira – dentre diferentes diários oficiais eletrônicos e jurisprudência – que envolviam o uso da LGPD, entre setembro de 2020 e setembro de 2022. Destacaram-se os Tribunais de Justiça dos Estados de São Paulo, Bahia e Rio Grande do Sul e o do Distrito Federal.

Ao acompanhar a evolução e amadurecimento da LGPD

no Brasil, observou-se que a LGPD foi mencionada em diferentes áreas do Direito, com destaque ao Direito do Consumidor, Civil e do Trabalho. E, em comparação com o seu primeiro ano de vigência, percebeu-se que a tendência de aplicação da LGPD só aumenta, considerando que em 2021 foram identificadas 274 decisões judiciais e, em 2022, 665 decisões nas quais se vislumbrou relevância na discussão envolvendo a LGPD.

Por fim, os temas mais recorrentes em que a LGPD foi discutida foram: (i) pedidos de provas digitais de geolocalização em ações trabalhistas; (ii) responsabilidade civil por incidentes de segurança e vazamento de dados; (iii) inscrição indevida em cadastro de inadimplentes da Serasa; e (iv) direito de revisão no tratamento automatizado de dados pessoais.

Autoridades.



MPF pretende investigar suposto apagão de arquivos no Planalto

Após notícias de que HDs de equipamentos da Presidência da República estariam sendo formatados por conta de suposta ameaça aos sistemas e bancos de dados, o Ministério Público Federal instaurou procedimento investigatório buscando apurar possível apagão de documentos dos computadores do Palácio do Planalto, alertando serem os fatos graves e suficientes para instaurar investigação.

O órgão ministerial solicita que a Secretaria-Geral explique quem determinou a formatação dos HDs e se foram apuradas possíveis causas e responsáveis pelo acontecimento. É sustentado, ainda, que a Presidência não esclareceu se computadores foram formatados, se arquivos foram danifica-

dos ou apagados, se dados sensíveis foram vazados, se dados públicos foram perdidos ou se houve investigação sobre a origem do ataque.

A Secretaria-Geral, por sua vez, garantiu que não houve vazamento de dados, nem comprometimento de sistemas hospedados na rede da Presidência da República, informando ter detectado “malware” em alguns computadores, que teria se originado em razão da prática de “phishing”.





Maioria dos órgãos públicos federais encontra-se inadequada à LGPD

Em acórdão recente, o TCU divulgou dados apurados em auditoria de 382 instituições públicas federais e concluiu que 76,7% das instituições encontram-se em um nível inexpressivo ou inicial de adequação à LGPD. Além disso, 82% das entidades não consideram os riscos de exposição a incidentes de segurança para tratar dados dos cidadãos brasileiros.

O resultado é surpreendente se considerado o fato de que a expectativa era de que as sanções administrativas da ANPD, que dependiam de Portaria específica a respeito da dosimetria das penas relacionadas à LGPD, comesçassem a ser aplicadas pela autoridade administrativa competente em outubro de 2022.

Além disso, releva considerar que o Brasil é vítima recorrente de ataques virtuais, como o que ocorreu em dezembro de 2020 contra o Ministério da Saúde (instituição citada no relatório do TCU).



Corregedorias gerais dos tribunais possuem prazo de 90 dias para comprovar adequação à LGPD

As corregedorias gerais dos Tribunais de Justiça dos Estados devem, no prazo de 90 dias, prestar esclarecimentos sobre a adequação à LGPD.

O que se busca é colocar em prática o Provimento nº 134/2022 da Corregedoria Nacional de Justiça, o qual dispõe sobre medidas que devem ser adotadas pelos cartórios extrajudiciais para adequação à mencionada lei. A título de exemplo, o Provimento dispõe que o responsável pelas serventias deve atentar a medidas de segurança técnicas e administrativas para proteger dados pessoais de acessos não autorizados ou situações acidentais ou ilícitas que possam violar o tratamento adequado aos dados.

A adequação é importante em razão da vulnerabilidade de informações que são prestadas aos agentes responsáveis pelos ofícios de registro civil de pessoas naturais.

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

**SÓCIAS RESPONSÁVEIS
PELO BOLETIM:**

Marcela Waksman Ejnisman

- Ⓔ Patrícia Helena Marta Martins
- Ⓔ Carla do Couto Hellu Battilana
- Ⓔ Bruna Borghi Tomé
- Ⓔ Luiza Sato
- Ⓔ Sofia Kilmar

Mais informações em:
tozzinifreire.com.br

**Tozzini
Freire.**
ADVOGADOS