

Tozzini Freire.

ADVOGADOS

BOLETIM

CYBERNEWS.

30ª Edição | 2023

Sumário

01

..... 03

..... 03

..... 04

..... 04

..... 05

02

..... 06

..... 08

..... 09

..... 10

03

..... 11

04

..... 12

05

13

..... 14



Realidade Brasileira.

Consulta pública sobre transferências internacionais de dados pessoais é aberta pela ANPD

No dia 15 de agosto, foi aberta consulta pública pela Autoridade Nacional de Proteção de Dados (ANPD) sobre a minuta de Resolução referente ao Regulamento de Transferências Internacionais de Dados Pessoais e do modelo de Cláusulas-Padrão Contratuais, em atenção aos artigos da Lei Geral de Proteção de Dados (LGPD): 33, II, alíneas a, b e c; 35, §§ 1º, 2º e 5º; e 36.

A consulta estará disponível até o dia 14 de setembro.

Consulta à sociedade sobre estudo preliminar a respeito do Legítimo Interesse é aberta pela ANPD

Foi aberta pela ANPD, no dia 16 de agosto, consulta à sociedade sobre Estudo Preliminar referente à hipótese legal de tratamento de dados pessoais do legítimo interesse, prevista no art. 7º, IX. da LGPD.

O estudo tem o objetivo de subsidiar o conteúdo do Guia Orientativo sobre a hipótese legal do legítimo interesse, a partir da junção da expertise técnica da Autoridade com a experiência prática dos agentes de tratamento sobre o tema.

Nova carteira de identidade vai usar blockchain

O governo federal decidiu adotar o sistema de autenticação e criptografia blockchain na nova carteira de identidade, que substituirá o número do Registro Geral (RG) pelo Cadastro de Pessoa Física (CPF) como número identificador único e com validade nacional.

A informação foi veiculada pelo secretário de Governo Digital do Ministério da Gestão e Inovação, Rogério Mascarenhas, que disse que a inovação visa prevenir falsificações, de modo a garantir a validade das informações.

Projeto de Lei propõe tornar obrigatória divulgação na mídia de incidentes de segurança com dados pessoais

Poderá tornar-se obrigatória a divulgação de incidentes de segurança que possam acarretar risco ou dano relevante aos titulares de dados pessoais em veículos de mídia de grande circulação, caso o Projeto de Lei (PL) nº 1.876/2023, de autoria do deputado federal Marcos Tavares, seja aprovado nas comissões temáticas de Comunicação e Constituição, Justiça e Cidadania.

A proposta também requererá que os agentes de tratamento divulguem informações sobre o incidente nas suas mídias sociais e perfis na internet, além do reporte já obrigatório à ANPD. O PL dá ao Poder Executivo a possibilidade de elaborar normas complementares para tornar efetiva a nova obrigação.

O autor do PL acredita que a medida será positiva para dar mais transparência sobre os incidentes de segurança.

Conselho Diretor da ANPD encaminha para a presidência da República lista de candidaturas para a 2ª formação do CNPD

Em 28 de julho, a ANPD compartilhou para a análise do presidente da República as listas tríplices formadas pelo Conselho Diretor da ANPD para a 2ª Formação do Conselho Nacional da Proteção de Dados (CNPD). Os novos conselheiros serão nomeados pela presidência no decorrer deste ano para o mandato de dois anos atuando em conjunto com a ANPD.

Vale ressaltar que o CNPD se estrutura como um órgão de aconselhamento vinculado à ANPD voltado para trazer a participação da sociedade civil e do setor público para as discussões realizadas no âmbito da Autoridade. Assim, o CNPD abriu candidaturas específicas para os seguintes grupos: (i) organizações da sociedade civil, (ii) instituições científicas, tecnológicas e de inovação, (iii) confederações sindicais, (iv) entidades representativas do setor empresarial e, ainda, (v) entidades representativas do setor laboral.

Dessa forma, o CNPD desempenha um papel relevante na moldagem de políticas e práticas relacionadas à proteção de dados pessoais e privacidade no Brasil, buscando, assim, garantir a implementação eficaz da LGPD em apoio direto à ANPD.



02

Poder Judiciário.

Empresas são condenadas por ataque hacker

Empresa operadora de máquina de cartão crédito é condenada por negligência na adoção de medidas de segurança. A decisão foi estabelecida pela 2ª Turma Recursal do Tribunal de Justiça de Santa Catarina (TJSC) devido à culpa concorrente em um ataque hacker.

De acordo com o alegado nos autos, em novembro de 2021, uma empresa que atua no segmento de atacado e varejo firmou contrato com uma empresa responsável pela gestão de máquinas de pagamento por cartão de crédito. Em 14 de janeiro de 2022, funcionários da empresa de atacado e varejo perceberam uma invasão em seus sistemas, resultando na transferência não autorizada de R\$ 3.900,00 para um indivíduo que não fazia parte dos colaboradores.

Diante de tal acontecimento, a empresa de atacado e varejo, vítima da invasão, entrou com uma ação de indenização por danos materiais contra a empresa operadora da máquina de cartão de crédito, buscando o reembolso da transferência indevida. A empresa responsável pela máquina, entretanto, alegou que a culpa era exclusivamente de terceiros que teriam invadido o sistema e contestou a aplicabilidade do Código de Defesa do Consumidor (CDC) ao caso.

O acórdão, por unanimidade, confirmou a sentença do Juizado Especial Cível de São Miguel do Oeste, que considerou que ambas as empresas tiveram culpa no

incidente. Como resultado, a empresa operadora das máquinas de cartão de crédito foi condenada a pagar metade do prejuízo, totalizando o valor de R\$ 1.950,00.

O TJSC observou que a empresa prejudicada demonstrou negligência ao não implementar um sistema de firewall adequado para proteger a rede e garantir a identificação de quem acessava o sistema. Além disso, entendeu que a segurança fornecida pelo sistema disponibilizado ficou abaixo do esperado, devido à utilização de senhas fracas e à falta de monitoramento específico dos protocolos de internet (IPs - número de identificação dos dispositivos conectados à internet).



Proteção de dados pessoais é responsabilidade tanto das empresas quanto dos consumidores

Juíza de Goiânia sentenciou que a proteção de dados exige cautela tanto das empresas, ao criarem políticas e medidas de segurança, quanto dos usuários, em manter seus dados pessoais e senhas protegidos.

O 5º Juizado Especial Cível de Goiânia negou o pedido indenizatório feito por consumidora que alegou que uma Companhia Aérea havia vazado seus dados pessoais.

A autora arguiu que a sua antiga união estável é objeto de um processo judicial e que seu ex-cônjuge trouxe aos autos desse processo, sem seu consentimento, informações sobre passagens de viagem que ela realizou para Portugal, o que violaria seus dados pessoais.

No entanto, a juíza Roberta Nasser Leone seguiu o entendimento de que houve descuido da própria autora. Isso porque, essas informações só poderiam ser obtidas a partir de seu login e senha, de forma que não há como provar qualquer vazamento de dados por parte da empresa ré.





TJSP afirma a inexistência de violação da LGPD quando há tratamento de dados públicos

Em acórdãos prolatados no final de julho e no início de agosto de 2023, o Tribunal de Justiça do Estado de São Paulo (TJSP) revelou entendimento que não há ocorrência de ato ilícito indenizável quando as informações contidas na base de dados são públicas e obtidas por meio lícito, tratadas para a proteção do crédito. A decisão está em consonância com o artigo 7º, inciso X da LGPD.

Além disso, o Tribunal também entendeu que quando os dados divulgados são meramente cadastrais, não configurando dados sensíveis, não há descumprimento do dever de informação, posto que não há necessidade de autorização ou comunicação do titular dos referidos dados pessoais.

O Superior Tribunal de Justiça (STJ) teve o mesmo entendimento em acórdão proferido em março de 2023. Na ocasião, foi julgado a inexistência de dano moral indenizável em hipótese de vazamento de dados meramente cadastrais e não sensíveis, como CPF e número de telefone, uma vez que são dados fornecidos corriqueiramente e que não teriam o condão de violar o direito de personalidade do titular de dados.

ANPD ajuíza ação civil pública para proteger sua identidade em prol do interesse comum

A ANPD ajuizou uma ação civil pública junto com o Instituto Nacional da Propriedade Industrial (INPI) contra a Associação Nacional dos Profissionais de Privacidade de Dados (ANPPD) e seu presidente, com o intuito de cessar o uso de nome, marca e sigla homófonas às suas.

Isso porque, segundo a ANPD, a utilização desses signos identificadores estaria confundindo empresas, profissionais e consumidores, tratando-se de propaganda enganosa. A associação acaba se passando por um ente público e, assim, apresenta um risco para a sociedade como um todo.

Além das irregularidades na identificação nominal e visual, a ANPPD também criou, sem autorização legal, um Registro Nacional de Profissionais de Privacidade de Dados e se coloca como homologadora de softwares de privacidade e de cursos de ensino sobre Proteção de Dados.

Após apurar as questões acima apontadas, o INPI entendeu pela nulidade do registro da sigla ANPPD, que havia sido realizado previamente. Ocorre que, como havia decorrido mais de 180 dias da expedição do registro, a nulidade não conseguiu mais ser declarada na esfera administrativa. Assim, buscou-se a tutela jurisdicional para que tais práticas lesivas sejam cessadas.

A tutela de urgência foi deferida para determinar que (i) seja suspensa a veiculação de propaganda a respeito do Registro Nacional de Profissionais de Privacidade e da respectiva Carteira de Registro Nacional dos Profissionais de Privacidade de Dados; (ii) a associação se abstenha de usar siglas e logos semelhantes aos da ANPD, ainda que na forma de identidade visual, bem como na denominação social da associação e nas mídias sociais e meios de comunicação vinculados à associação e aos membros da diretorias (inclusive com modificação e/ou remoção das publicações anteriores); e (iii) a associação se abstenha do uso do nome de domínio anppd.org, o qual deveria ser alterado em 120 dias.

Nessa decisão, o magistrado reconheceu que de fato são perceptíveis as semelhanças entre os signos identificadores da ANPD e da ANPPD, seja pelas siglas, pelas cores utilizadas ou pela correspondência de áreas de atuação, o que pode gerar confusão e danos ao mercado, justificando, portanto, o deferimento da tutela antecipada para a suspensão da utilização de siglas e logos semelhantes.

03 Autoridades.

Estado de Goiás apresenta Projeto de Lei para impedir que estabelecimentos solicitem dados pessoais do consumidor para vendas

A Assembleia Legislativa do Estado de Goiás estuda a aprovação de PL nº 600/2023 que busca impedir que os estabelecimentos comerciais exijam o fornecimento de dados pessoais dos consumidores como condição para a venda ou prestação de serviços.

Nos termos do projeto, “é vedado ao estabelecimento comercial ou de serviços condicionar a venda de produto ou a prestação de serviço ao fornecimento de dados pessoais pelo consumidor, salvo nos casos em que a obrigatoriedade do fornecimento estiver prevista em lei”. A matéria foi aprovada pela Comissão de Constituição e Justiça (CCJ) e será votada em plenário.

Pela proposta, de autoria do deputado estadual Vetter Martins, o descumprimento da medida sujeitaria os infratores às sanções previstas no CDC, exceto nos casos em que o fornecimento seja obrigatório por lei.

Justificando o PL, o parlamentar afirma que a previsão busca trazer mais clareza aos consumidores, além de estar em consonância com as diretrizes da LGPD.

021

Avanços Normativos.

CNI publica um guia de boas práticas de proteção de dados pessoais para aplicação em indústrias

A Confederação Nacional da Indústria (CNI) publicou um extenso guia de boas práticas de proteção de dados pessoais para aplicação em processos das indústrias ([acesse aqui](#)). Além disso, destacou que a implementação da cultura de proteção de dados em indústrias aumenta a fidelização e confiança com clientes, amplia oportunidades de negócios envolvendo dados pessoais e auxilia no cumprimento de exigências legais.

Com o objetivo de estimular e auxiliar as indústrias a se adequarem à LGPD, o Guia destaca os principais conceitos e princípios da LGPD, exemplifica processos e tipos de dados pessoais tratados pelo setor da indústria, bem como fornece diversos protocolos gerais para cada uma das etapas do tratamento de dados, desde a coleta até a eliminação. Além disso, apresenta protocolos específicos para a área de marketing das indústrias, transferência internacional de dados, e para o cumprimento de obrigações legais da LGPD, como a elaboração de relatórios de impacto e garantia dos direitos dos titulares.

05 Cenário Internacional.

Autoridade de Proteção de Dados Francesa multa Criteo em €40.000.000

Em 15 de junho de 2023, a Autoridade Francesa de Proteção de Dados (CNIL, na sigla em francês) multou, em 40 milhões de Euros, uma empresa de publicidade online especializada em retargeting comportamental (rastreamento da navegação de usuários por meio de cookies para exibir propagandas personalizadas). A decisão foi tomada porque a empresa não cumpriu com o Regulamento Geral de Proteção de Dados (GDPR, na sigla em inglês). Essa multa é o resultado de uma investigação da CNIL sobre a ausência de coleta de consentimento dos titulares pela Criteo.

Além disso, a Criteo descumpriu outros dispositivos do GDPR sobre os deveres de informação e transparência, garantia do direito do titular de acesso, revogação do consentimento e eliminação de dados, e ausência de celebração de acordo entre os co-controladores dos dados (artigos 7.1, 7.3, 12, 13, 15.1, 17.1 e 26).



Índia aprova nova lei de proteção de dados digitais

A Índia aprovou, no início de agosto, a nova lei de proteção de dados pessoais digitais que estabelece normas e procedimentos sobre tratamento de dados pessoais realizados por empresas de tecnologia.

Dentre suas disposições, a lei, em suma: (i) atribui ao governo da Índia poderes para isentar as agências estatais da lei, bem como o poder de buscar informações de empresas de tecnologia e requerer o bloqueio de conteúdos; (ii) fornece aos usuários o direito de corrigir ou apagar seus dados pessoais; e (iii) permite que empresas de tecnologia transfiram dados de alguns usuários para o exterior.

Além disso, propõe penalidades equivalentes de até US\$ 30 milhões para casos de violações e descumprimento da lei.






A lei sofreu algumas críticas de opositores que alegam que a lei resulta em uma vigilância ampla e afeta a liberdade de imprensa, bem como dilui a lei de direito à informação da Índia.



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