TF cybernews
TOZZINIFREIRE ADVOGADOS
4ª edição | 2020

Realidade Brasileira

Lançado o portal da Autoridade Nacional de Proteção de Dados

Já está no ar o portal da Autoridade Nacional de Proteção de Dados (ANPD), que é o órgão responsável por elaborar as diretrizes para a Política Nacional de Proteção de Dados, promover na população o conhecimento das normas e das políticas públicas e das medidas de segurança, promover e elaborar estudos sobre as práticas nacionais e internacionais de proteção de dados, estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados e fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação – o que tende a contribuir para uma maior segurança jurídica, de acordo com a própria ANPD.

O portal traz a estrutura regimental da Autoridade, apresentando-a como órgão da Presidência da República, e as disposições sobre o Conselho Diretor, como órgão máximo de direção do órgão. A página ainda apresenta as coordenações-gerais de regulação, fiscalização e tecnologia e pesquisa.

A página, que pode ser acessada pelo endereço "www.gov.br/anpd", disponibiliza também os canais de atendimento da ANPD, pelos quais se pode realizar denúncias, solicitações, sugestões e elogios. O portal traz ainda conteúdo sobre a estrutura organizacional e a composição do Conselho Diretor e o rol de competências da ANPD – estabelecido pelo art. 55-J da LGPD –, além da agenda dos diretores da Autoridade. Finalmente, o site disponibilizou recentemente documento contendo respostas a "Perguntas Frequentes" sobre o escopo e função da LGPD e os principais conceitos da lei.

Orientações Gerais

As recomendações do Comitê Europeu sobre a transferência internacional de dados

O Comitê Europeu para a Proteção de Dados (EDPB) emitiu as "Recomendações 01/2020", no dia 10 de novembro de 2020, sobre as ferramentas para garantir o nível de proteção de dados pessoais, nas transferências internacionais. Essas recomendações fornecem aos exportadores de dados uma série de etapas a serem seguidas, fontes de informações e alguns exemplos de medidas complementares que podem ser implementadas.

Preliminarmente, como primeira etapa, recomenda-se aos exportadores o mapeamento de todas as transferências internacionais de dados pessoais. Deve-se verificar também se os dados transferidos são adequados e relevantes para os fins para os quais foram transferidos e processados. A segunda etapa é verificar a ferramenta da qual depende a transferência e se o país para o qual se transferirá os dados apresenta um alto nível de adequação.

Em seguida, como terceira etapa, deve-se avaliar se há algo na lei ou nas práticas adotadas no país que receberá os dados transferidos que possa interferir na eficácia das ferramentas de proteção da transferência. Para avaliar tais elementos, deve-se analisar a legislação do país que trata do acesso aos dados pelas autoridades públicas. Na ausência de legislação, deve-se verificar outros fatores objetivos, como a probabilidade de essas autoridades terem acesso aos dados pessoais.

A quarta etapa é identificar e adotar medidas complementares necessárias para elevar o nível de proteção dos dados transferidos. Essa etapa só é necessária se a avaliação revelar que a legislação de um país teria o potencial de afetar a eficácia das ferramentas de transferência. Nos casos em que nenhuma medida complementar seja adequada, recomenda-se evitar, suspender ou encerrar a transferência, a fim de evitar o comprometimento do nível de proteção dos dados pessoais.

A quinta etapa é tomar todas as medidas formais necessárias para validar referidas medidas complementares, como consultar as autoridades nacionais de proteção de dados envolvidas. Por fim, a sexta e última etapa é reavaliar, de tempos em tempos, o nível de proteção concedido aos dados transferidos e monitorar se houve ou haverá qualquer evolução que possa afetá-los.

Avanços Normativos

Reflexos da LGPD no âmbito estadual: princípio da finalidade no contexto dos cadastros em farmácias

Em 02 de dezembro foi publicada no Diário Oficial do estado de São Paulo a Lei Estadual nº 17.301/2020, norma que proíbe farmácias e drogarias de exigir o CPF dos seus consumidores, no ato da compra, sem informar de forma adequada e clara sobre a concessão de descontos

Originalmente proposta pelo deputado estadual Alex de Madureira (PSD), a Lei Estadual tem como foco assegurar que os consumidores de farmácias, enquanto titulares dos dados usados para a abertura de cadastro e concessão de promoções, tenham acesso a informações claras e adequadas sobre a finalidade que será dada para o uso do CPF (seu dado pessoal) coletado no ato das compras. Em complemento a esta disposição, a norma estabelece que na hipótese de coleta deste dado dos titulares sem a apresentação das informações necessárias, a farmácia será sancionada com multa de 200 (duzentas) Unidades Fiscais do Estado de São Paulo (o que pelo índice de 2020 corresponde a aproximadamente R$ 5.500).

Vale ressaltar que o objeto desta proposta já encontra amparo no âmbito das garantias gerais da Lei Geral de Proteção de Dados. Nesse sentido, à luz do previsto na LGPD, a finalidade dada pelas farmácias para a coleta do dado de CPF dos titulares deve ser disponibilizada de forma clara e adequada aos titulares (em atenção ao dever de prestação de informação dos agentes de tratamento, previsto no art. 9º da LGPD). Reforçando este direito dos titulares, a LGPD ainda estabelece enquanto princípio que o tratamento de dados pessoais deve ser feito para propósitos "específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades" (em atenção ao princípio da finalidade, previsto em seu art. 6º).

Projeto de Lei nº 5.141/2020 é apresentado propondo a redução do escopo de aplicação da LGPD para dados tratados com fins religiosos

A atual redação da Lei Geral de Proteção de Dados já contempla hipóteses específicas de tratamento de dados que fogem do seu escopo de aplicação, o que inclui cenários tais como aqueles de uso dos dados pessoais para fins jornalísticos ou artísticos. Com o intuito de ampliar este rol taxativo, o Projeto de Lei nº 5.141/2020, de autoria do deputado Alex Santana (PDT/BA) foi apresentado em 20 de novembro de 2020 propondo que o tratamento de dados para fins religiosos também fique fora do escopo de aplicação da LGPD.

Segundo o autor do Projeto, há uma necessidade de estender as hipóteses de não aplicabilidade da LGPD para os procedimentos adotados pelas organizações religiosas ao campo religioso visando assegurar o livre exercício dos cultos religiosos, incluindo as suas liturgias e seus procedimentos internos. Em paralelo a esta proposta, entretanto, vale ressaltar que dados pessoais referentes a convicção ou ainda aqueles a respeito de filiação a organização de caráter religioso, enquanto dados pessoais classificados como sensíveis, recebem atualmente proteção especial na LGPD em razão do potencial discriminatório que pode vir a recair sobre seus titulares em função do tratamento dessas informações pessoais.

Em meio a esse contexto, o Projeto de Lei aguarda despacho do presidente da Câmara dos Deputados para seguir tramitação.

Novos parâmetros para a seleção do Encarregado: o que a experiência da Administração Pública pode elucidar?

O processo de seleção de Encarregados na Administração ganhou destaque em outubro de 2020, com a Instrução Normativa (IN) nº 100/2020, a qual dispõe sobre a indicação do Encarregado pelo Tratamento dos Dados Pessoais nos órgãos do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP). Passado um mês da publicação desta Instrução, a Secretaria Especial de Desburocratização, Gestão e Governo Digital do Ministério da Economia apresentou a IN nº 117/2020 dispondo sobre a indicação do Encarregado no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional.

Na medida em que o Encarregado (ou DPO) é uma figura central para qualquer organização (seja ela pública ou privada) ao atuar como elo de contato entre a instituição e seus titulares, a seleção da pessoa física ou jurídica que assumirá esta posição demanda cautela. No âmbito da Administração Pública Direta, a IN nº 117/2020 determina que o Encarregado deverá: (i) "possuir conhecimentos multidisciplinares essenciais à sua atribuição, preferencialmente os relativos aos temas de: privacidade e proteção de dados pessoais, análise jurídica, gestão de riscos, governança de dados e acesso à informação no setor público" e ainda (ii) "não deverá se encontrar lotado nas unidades de Tecnologia da Informação ou ser gestor responsável de sistemas de informação do órgão ou da entidade".

Nesse sentido, a IN nº 117/2020 estabelece diretrizes sobre pré-requisitos que devem ser observados na seleção do Encarregado, prezando por um caráter multidisciplinar de suas competências. Desse modo, a Administração Pública não busca um DPO que tenha exclusivamente um repertório técnico, enfatizando de fato a necessidade de maior contato de sua parte com o âmbito tanto jurídico quanto gerencial do contexto do tratamento de dados pessoais. De forma análoga, ressalvadas as devidas peculiaridades dos setores público e privado, é possível avaliar que a atuação multidisciplinar do Encarregado no campo privado também demandará maior contato por parte destes indivíduos com a intersecção entre o aspecto jurídico da proteção de dados com questões técnicas e gerenciais dos respectivos negócios em que atuam, trazendo assim as premissas da IN nº 117/2020 como relevantes estratégias para a otimização da atuação dos futuros DPOs também do mercado privado.

Poder Judiciário

TRF-1 sofre ataque hacker

Na sequência dos ataques hackers sofridos pelo STJ e outros órgãos e tribunais no país no início de novembro, outro tribunal sofreu ataque em 27/11 deste ano: o TRF-1.

O ataque hacker fez com que o Tribunal retirasse do ar o portal da Justiça Federal do Distrito Federal e de mais outros 13 estados: Acre, Amazonas, Roraima, Rondônia, Amapá, Pará, Mato Grosso, Tocantins, Maranhão, Piauí, Bahia, Minas Gerais e Goiás.

O TRF-1 é o tribunal que possui o maior acervo da Justiça Federal, abrangendo 66% do território nacional. O mencionado ataque expôs dados sensíveis de mais de 40 bases de dados do tribunal.

Em nota, o Tribunal afirmou que, por prevenção e para permitir adequada investigação, colocou os seus sistemas em modo restrito. Em razão disso, os usuários externos do tribunal ficaram completamente sem acesso aos sistemas do TRF-1. Contudo, já no dia 28/11, o tribunal informou que iniciaria, de forma gradativa, o restabelecimento dos serviços de informática para acesso externo, assim que fosse garantida a segurança adequada.

Além disso, o Tribunal esclareceu que sua equipe de resposta a incidentes de segurança está trabalhando para revisar as eventuais vulnerabilidades dos serviços e sistemas. Considerando a gravidade do ocorrido, o TRF-1 informou que adotou as medidas jurídicas cabíveis para a apuração dos fatos.

Justiça Eleitoral decide sobre uso de banco de dados públicos

A Justiça Eleitoral do Espírito Santo deferiu medida liminar para impedir que um filiado ao partido PCdoB envie mensagens aos seus eleitores, pois teria se aproveitado de seu cargo público para ter acesso ao banco de dados do departamento de recursos humanos da Secretaria Estadual de Saúde, obtendo os dados pessoais dos funcionários do estado.

A decisão não foi fundamentada na Lei Geral de Proteção de Dados, mas, sim, no art. 57-E da Lei nº 9.504/1997, que veda aos órgãos da administração pública direta e indireta a utilização, doação ou cessão de cadastro eletrônico de seus usuários, em favor de candidatos, partidos ou coligações. Contudo, desde já, podemos ver uma sinalização do Judiciário para entender como ilegal o uso de bancos de dados públicos para finalidades diversas das quais esses dados foram primeiramente coletados.

Na mesma linha, o TSE já havia decidido que o Conselho Regional de Medicina do Estado de Goiás, que utilizou seu cadastro de associados para, via mensagem eletrônica, manifestar posição política contrária a uma candidata, também estaria vedado de usar seus cadastros eletrônicos em favor de candidatos, partidos ou coligação.

Embora essas decisões tenham sido proferidas com base na legislação eleitoral, é possível fazer um paralelo com o que dispõe a LGPD, que também poderia ser utilizada como fundamento para a vedação do uso de cadastros eletrônicos em favor de candidatos ou partidos. Isso porque a obtenção de e-mails de eleitores através do uso de cadastro eletrônico próprio ou compra de banco de dados para a utilização em propaganda eleitoral, sem consentimento expresso dos titulares dos dados para essa finalidade específica, não estaria de acordo com a LGPD, que prevê que o tratamento de dados pessoais somente poderá ser realizado para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades (art. 6º, I, da LGPD).

STJ cria página especial dedicada à LGPD

Em atendimento à recomendação nº 73/2020 do Conselho Nacional de Justiça, o Superior Tribunal de Justiça (STJ) lançou, no dia 30 de novembro de 2020, uma página especial em seu site dedicada a informar aos cidadãos a respeito das regras e previsões contidas na Lei Geral de Proteção de Dados. O portal pode ser consultado por meio do seguinte endereço eletrônico: https://www.stj.jus.br/sites/portalp/WebPub/NovoPortal/LGPD.aspx.

Na data de lançamento do portal, o ministro Humberto Martins, atual presidente do STJ, declarou que a Corte já está se adequando aos direitos subjetivos previstos na lei, entendendo que os meios de controle internos do Poder Judiciário são eficientes para garanti-los. Ainda, afirma que em atendimento ao princípio da transparência e segurança da informação, o STJ já vem adotando medidas para garantir o pleno cumprimento das disposições da lei, inclusive com a instituição de comissão para coordenar as ações necessárias pelo órgão.

O portal é resultado, portanto, da atuação do STJ em garantir a maior transparência à população, orientando-a sobre seus direitos, bem como sobre a atuação da Corte para a implementação da lei – o que tem sido feito pela comissão instituída para identificar as ações necessárias para a implementação da LGPD no Tribunal, conforme dispõe a Portaria STJ/DG nº 590/2020.

A página, de fácil consulta e visualização, contempla também um glossário com todos os termos mais relevantes da lei, bem como mantém atualizadas as informações acerca de todos os eventos e ações implementadas pelo STJ sobre o tema.

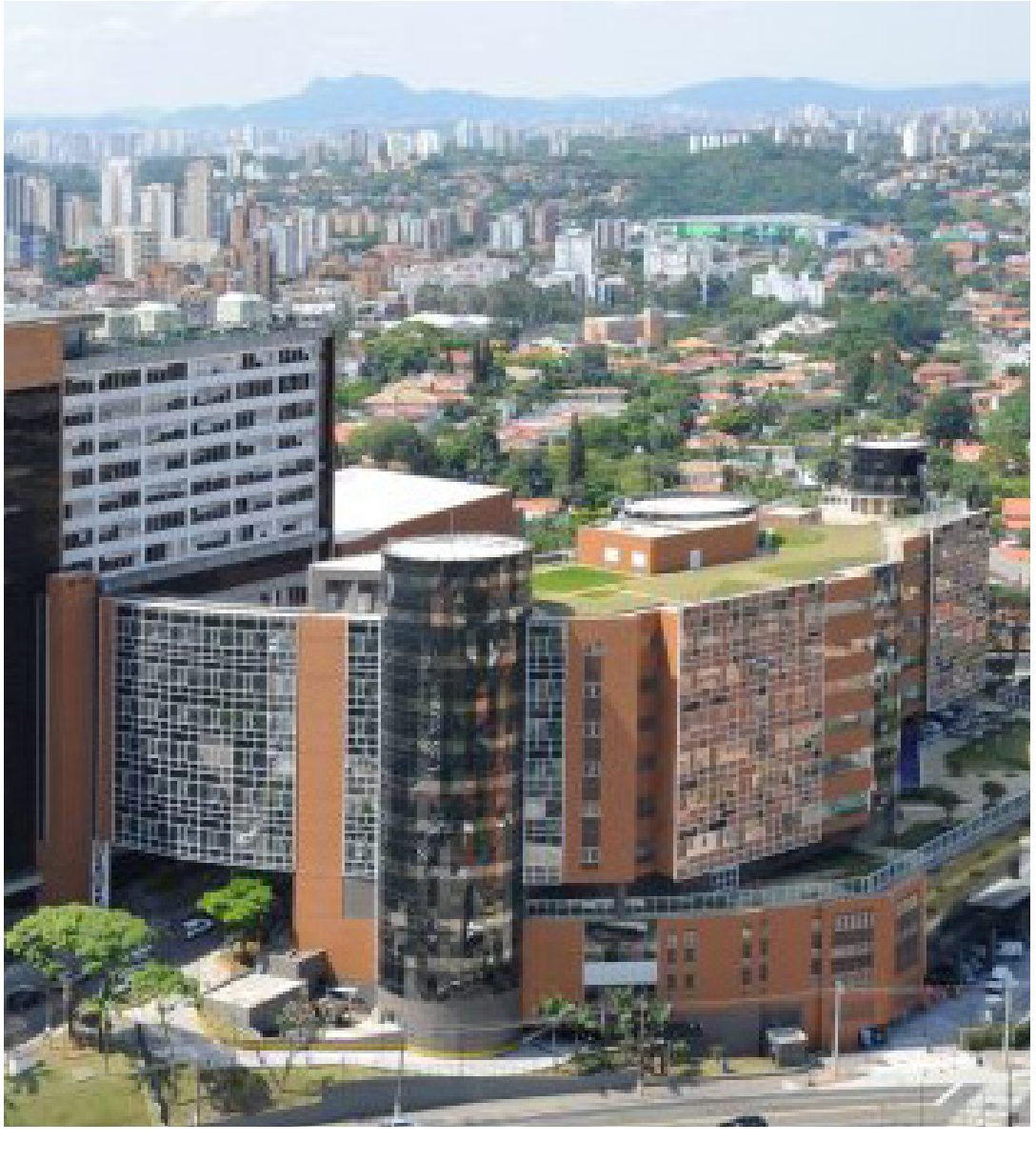
Justiça Eleitoral do Distrito Federal autoriza quebra do sigilo de dados dos suspeitos de invasão ao sistema do TSE

Após operação iniciada pela Polícia Federal para investigar o ataque hacker sofrido pelo Tribunal Superior Eleitoral (TSE) em 15 de novembro de 2020, data do primeiro turno das eleições municipais de 2020 e que ocasionou a divulgação ilegal de dados de servidores públicos do tribunal, a magistrada Geilza Diniz, da 1ª Vara Eleitoral do Distrito Federal, autorizou a quebra do sigilo de dados – em endereços de e-mail – de três brasileiros considerados suspeitos pela invasão.

Nesta mesma decisão, foi ordenada a busca e apreensão de documentos, roteadores de internet, bem como dispositivos eletrônicos que armazenam dados, tudo com o intuito de instruir a investigação e buscar desarticular eventual ação de grupo de hackers.

Há suspeita de que um grupo formado por jovens brasileiros e portugueses teria atuado em sete tentativas de acesso ao site do TSE, o que pode, inclusive, ter provocado a instabilidade do aplicativo "e-título" utilizado por eleitores no dia da votação para justificar a eventual ausência.

Proteção ao Consumidor



PROCON-SP notifica Hospital Albert Einstein por suposto vazamento de dados

O PROCON-SP pediu esclarecimentos ao Hospital Albert Einstein a respeito de suposto vazamento de informações pessoais e médicas de pacientes testados, diagnosticados e internados pela COVID-19.

Um funcionário do hospital, trabalhando em um projeto com o Ministério da Saúde, teria divulgado na internet lista de senhas do sistema do Ministério da Saúde que dava acesso aos bancos de dados dos pacientes, expondo informações de ao menos 16 milhões de pessoas.

Os esclarecimentos pedidos pelo PROCON-SP relacionam-se à adoção de medidas de segurança para proteção de dados pessoais, à qualificação dos funcionários e colaboradores do hospital a respeito da Lei Geral de Proteção de Dados, aos procedimentos adotados para análise de um incidente com dados pessoais, às medidas de segurança de dados, às medidas práticas de contenção de danos e ao protocolo de prevenção de vazamento de dados. Por fim, o PROCON-SP ainda requereu esclarecimentos a respeito das medidas de segurança adotadas no processo de digitalização do prontuário médico e exame dos pacientes e sobre se haveria alguma forma de criptografia das informações dos pacientes e usuários dos serviços laboratoriais.

O Instituto de Defesa do Consumidor (IDEC) pediu ao Ministério Público Federal (MPF) que iniciasse inquérito visando à investigação desses fatos, bem como requerendo pedido de informações ao Ministério da Saúde para maior detalhamento sobre a parceria com o hospital que possibilitava o acesso de funcionários do hospital a dados pessoais. Ainda não há notícia a respeito do início dessa investigação formalmente.

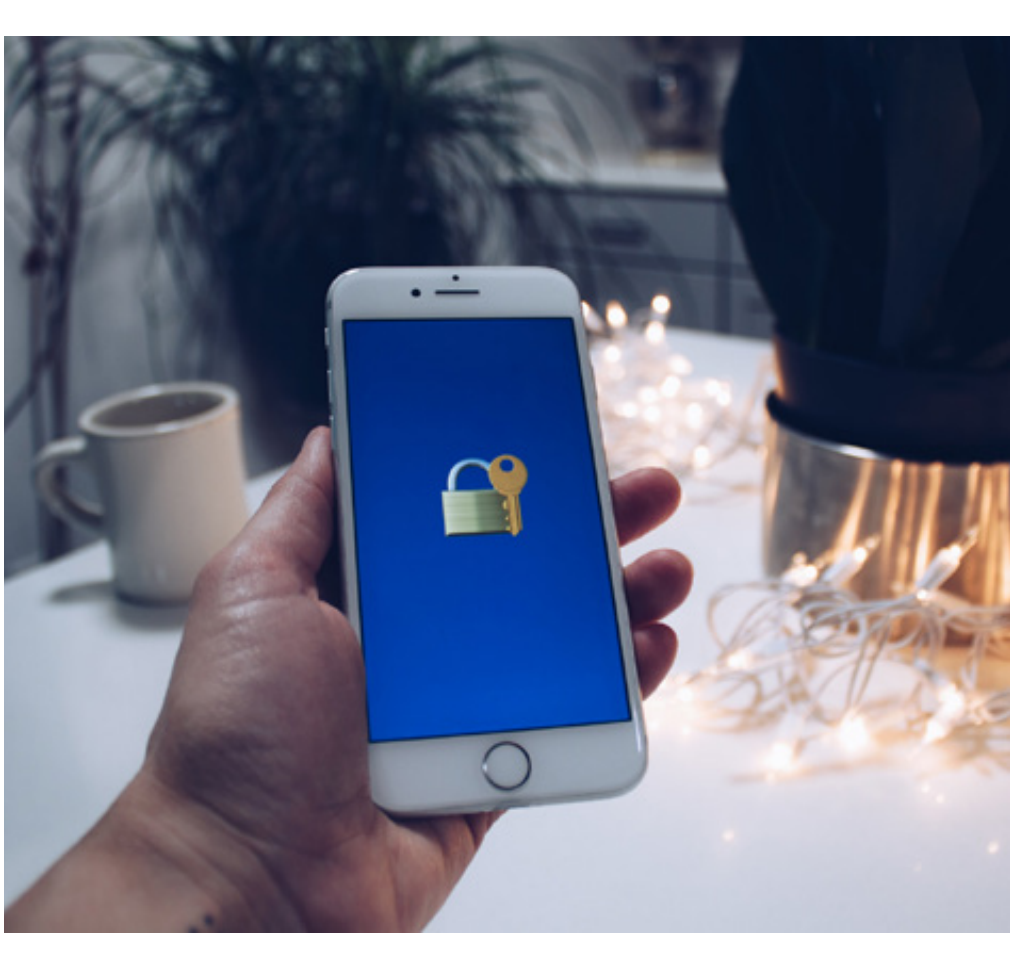
Essa notícia mostra com clareza que, embora em um primeiro momento possa se entender que proteção de dados seria um tema mais próximo de empresas de tecnologia, a realidade é que a proteção de dados envolve todas as empresas e órgãos que possuam bases de dados, especialmente hospitais que coletam dados relativos à saúde de seus pacientes, os quais são tidos como dados pessoais sensíveis, nos termos do art. 5º, II, da Lei Geral de Proteção de Dados.

Ministério Público

MPDFT obtém liminar que suspende a comercialização de dados pessoais pela Serasa Experian

A Unidade Especial de Proteção de Dados e Inteligência Artificial (ESPEC) do Ministério Público do Distrito Federal e Territórios (MPDFT) apurou ailegada comercialização de dados pessoais pela Serasa Experian. Segundo o levantamento do MPDFT, havia no banco de dados da referida empresa ofertado ao mercado cerca de 150 milhões de números de CPF de consumidores brasileiros, entre outros dados pessoais diversos, tais como nome e número de telefone. Diante disso, o MPDFT propôs a ação civil pública nº 0736634-81.2020.8.07.0001, visando a obrigar a cessar a referida prática de comercialização imediatamente (inclusive com pedido liminar específico nesse sentido), sem, contudo, pleitear indenização por danos morais coletivos.

A medida liminar pretendida restou indeferida, sob o argumento de que os dados pessoais comercializados pela Serasa Experian seriam constantemente fornecidos por consumidores, voluntariamente, em sua vivência no mercado de consumo. O MPDFT interpôs, então, agravo de instrumento e, em segunda instância, obteve a antecipação dos efeitos da tutela recursal para a imediata suspensão da comercialização dos dados pessoais de consumidores brasileiros pela Serasa Experian. Até o presente momento, a empresa não apresentou manifestação nos mencionados autos.



Decisões Internacionais

Autoridade de proteção de dados estoniana veda a exibição de prescrições médicas sem consentimento prévio do titular em plataformas de e-pharmacy

A autoridade de proteção de dados da Estônia deu o prazo de um dia para três redes de farmácias interromperem a exibição, para terceiros, de prescrições médicas de suas plataformas online, que teria sido realizada sem o consentimento prévio dos titulares, além da penalidade de 100 mil euros.

A autoridade estoniana entendeu que não há base legal para tal divulgação. Por mais que uma das redes de farmácia exigisse confirmação prévia e genérica dos titulares para que terceiros pudessem acessar a prescrição, essa confirmação não equivaleria ao consentimento prévio e voluntário do titular da prescrição médica. Isto porque, apenas pela confirmação, a rede de farmácia não é capaz de verificar para qual finalidade o terceiro poderá acessar as informações, nem se o consentimento foi dado voluntariamente.

Vale notar que, à luz da LGPD, apenas a manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada deve ser considerada consentimento válido. Para ser enquadrado como base legal de tratamento de dados, o consentimento deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular. A LGPD considera, por fim, nulas as autorizações genéricas para o tratamento de dados pessoais, uma vez que o consentimento deve se referir a finalidades específicas.

Carrefour France e Carrefour Banque sancionadas por série de infrações às normas da GDPR

A autoridade francesa de proteção de dados (*Commission Nationale de l'Informatique et des Libertés* ou CNIL) aplicou multa à Carrefour France e ao Carrefour Banque após receber várias reclamações contra o Grupo Carrefour. A CNIL verificou infrações nos tratamentos de dados de clientes e potenciais clientes da rede Carrefour relacionadas:

(I) à obrigação de informar os titulares de dados no momento da coleta de seus dados realizada nos sites *carrefour.fr* e *carrefour-banque.fr*, em razão da dificuldade de acesso às informações claras e suficientes sobre tratamento de dados;

(II) a cookies, os quais eram depositados automaticamente nos computadores dos usuários sem consentimento prévio;

(III) à obrigação de armazenar dados por tempo limitado;

(IV) ao dever de facilitar o exercício dos direitos dos titulares de dados; e

(V) princípio da legalidade e transparência nos tratamentos de dados, em razão da transferência de diversos dados, como endereço postal e número de telefone, por parte do Carrefour Banque, em descompasso ao que havia sido informado aos seus clientes que aceitavam o programa de fidelidade da Carrefour.

Vale notar que a LGPD dispõe sobre a necessidade do acesso facilitado às informações sobre o tratamento de seus dados, tais como: finalidade específica do tratamento; forma e duração do tratamento; identificação do controlador e informações de seu contato; informações sobre uso compartilhado de dados pelo controlador e a finalidade; entre outras informações, as quais deverão ser informadas aos titulares de dados assim que qualquer tratamento de dados pessoais for realizado.

Sanções milionárias por uso de cookies publicitários sem consentimento dos usuários e informação clara e suficiente

A *Commission Nationale de l'Informatique et des Libertés* (CNIL), autoridade francesa de proteção de dados, sancionou, no começo de dezembro, a Amazon Europe Core por depositar cookies* publicitários nos computadores de visitantes do site amazon.fr, sem prévio consentimento e informação clara e suficiente sobre os cookies.

Em investigação a CNIL apurou que os cookies, em sua maioria de fins publicitários, eram depositados automaticamente e instantaneamente nos computadores assim que seus usuários acessavam ao site da Amazon France. A autoridade entendeu que o aviso "Ao utilizar este site, você aceita a nossa utilização de cookies para oferecer e melhorar nossos serviços" apenas continha uma descrição genérica e aproximativa das finalidades dos cookies. Além disso, apontou a CNIL que o aviso, além de não especificar a finalidade do cookie, não apontava o direito do usuário de recusar o depósito dos cookies e como fazer isso.

Para a aplicação da sanção de 35 milhões de euros, a CNIL levou em conta as disposições do artigo 82 da Lei de Informação e Liberdades francesa, a qual prevê o direito dos usuários de serviços de comunicação eletrônicos de serem informados de maneira clara e completa sobre a finalidade de todas as ações destinadas a acessar informações em algum equipamento eletrônico de comunicação ou de registrar informações nesse equipamento, bem como sobre os meios pelos quais os usuários podem se opor.

Pelos mesmos motivos que a Amazon Europe Core, a Google LLC e a Google Ireland Limited foram sancionadas pela CNIL em 100 milhões de euros pelo depósito de cookies publicitários no mecanismo de pesquisa do site google.fr.

No cenário brasileiro, a Lei Geral de Proteção de Dados (LGPD) também prevê o direito do titular ao acesso facilitado às informações sobre o tratamento de seus dados, as quais deverão ser disponibilizadas de forma clara, adequada e ostensiva. Considerando os cookies como meios de coleta de dados pessoais, a utilização destes pequenos textos também deve observar as disposições da LGPD.

** pequenos textos que se hospedam em computadores, cujos objetivos principais são armazenar ou coletar informações, mas, especialmente, monitorar a atividade dos usuários na rede.*

EXTRAS

Ataque cibernético à EMBRAER

A EMBRAER informou no dia 30/11/2020 ter sofrido um ataque cibernético em seus sistemas de tecnologia da informação, que teria resultado na divulgação de dados supostamente atribuídos à companhia, como fotos, planilhas e documentos relacionados à venda do avião militar Super Tucano. O referido ataque teria sido identificado em 25/11/2020, indisponibilizando o acesso a apenas um único ambiente de arquivos da companhia. O evento fez com que a empresa interrompesse parcialmente os seus sistemas internos, impactando temporariamente algumas operações.

Em comunicado à imprensa, a EMBRAER informou estar investigando as circunstâncias do ataque, a fim de avaliar se existem impactos sobre seus negócios e terceiros, e determinar as medidas a serem tomadas.

Vazamento de dados pessoais de mais de 200 milhões de indivíduos com cadastro perante o Ministério da Saúde

Em uma segunda falha de segurança no sistema de notificações de COVID-19 do Ministério da Saúde – a primeira foi o vazamento de dados de 16 milhões de pessoas por conta de um erro de funcionário do Hospital Albert Einstein –, houve a exposição por pelo menos seis meses de dados pessoais de mais de 200 milhões de pessoas, uma vez que esses dados estavam disponíveis para consulta no site do Ministério.

Entre os dados disponíveis, constavam número do CPF, nome completo, endereço e telefone de indivíduos.

O problema foi causado pela exposição indevida de login e senha de acesso ao sistema que armazena os dados cadastrais de todos os brasileiros no Ministério da Saúde, tornando mencionado login e senha acessíveis por meio de um browser de internet comum.

O Ministério da Saúde informou que o problema identificado já teria sido corrigido, estaria investigando as responsabilidades pelo vazamento e tomando medidas para evitar sua repetição, e que possuiria protocolos de segurança e proteção de dados para mitigação dos riscos de exposição de dados.

O Conselho Nacional de Saúde solicitou esclarecimentos ao Ministério da Saúde sobre o fato e, também, acompanhamento e investigação pelo Ministério Público da União. Ainda não há notícia a respeito do início dessa investigação formalmente.

A comissão da Câmara de Deputados que acompanha as ações de enfrentamento à COVID-19 convocou uma audiência pública para que o Ministério da Saúde explicasse esse vazamento de dados, a requerimento do deputado federal e ex-ministro da Saúde Alexandre Padilha (PT). A audiência pública ainda não foi agendada.

O caso é mais um exemplo de que a proteção de dados pessoais não é uma obrigação exclusiva de empresas, mas também de órgãos públicos, como previsto pelo artigo 1º da Lei Geral de Proteção de Dados.

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

SÓCIAS RESPONSÁVEIS PELO BOLETIM:

- Marcela Waksman Ejnisman
- Bruna Borghi Tomé
- Carla do Couto Hellu Battilana
- Patrícia Helena Marta Martins

Mais informações em: tozzinifreire.com.br/

TOZZINIFREIRE ADVOGADOS