TF cybernews

3ª edição | 2020

TozziniFreire Advogados

Realidade Brasileira

A importância da ANPD para a visibilidade internacional do Brasil no cenário da proteção de dados

A LGPD estabeleceu a Autoridade Nacional de Proteção de Dados (ANPD) como a autoridade responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional, bem como de aplicar as penalidades administrativas previstas na lei. A ANPD também terá a incumbência de editar regulamentos sobre disposições da LGPD ainda não totalmente definidas, incluindo a necessidade e os requisitos da apresentação de relatórios de impacto à proteção de dados pessoais (também conhecidos como DPIAs), padrões e técnicas utilizados em processos de anonimização de dados pessoais, orientações sobre a atuação de agentes de tratamento na ocorrência de incidentes de segurança envolvendo dados pessoais, transferência internacional de dados, entre outros pontos.

Tendo em vista que caberá à ANPD a fiscalização da lei, a instrução dos processos administrativos e a aplicação das sanções previstas na LGPD, inclusive para agentes de tratamento de dados que sejam parte do poder público, é essencial que a ANPD tenha autonomia e independência para atuar livremente nos interesses da proteção de dados.

Neste sentido, a Organização para a Cooperação e Desenvolvimento Econômico (OCDE) recomendou, em um relatório que analisa a transformação digital e o setor brasileiro de telecomunicações, que o Brasil assegure, através da reavaliação do art. 55-A da LGPD, a total independência da ANPD, que, atualmente, vincula-se à Presidência da República, como órgão da administração pública.

Segundo o relatório, a LGPD gera uma importante confiança, que é essencial para a transformação digital. No entanto, é essencial assegurar uma Autoridade Nacional de Proteção de Dados independente, por meio de nomeações transparentes e justas, com base nos conhecimentos técnicos dos indicados aos cargos do Conselho de Administração, além de estabelecer um orçamento adequado à Autoridade (ponto também recomendado pelo relatório da OCDE).

As recomendações da OCDE têm a preocupação de garantir a independência da Autoridade para que possa desempenhar suas funções de defesa da privacidade e proteção de dados pessoais da forma mais adequada possível. Cumpre destacar que o grau de independência da ANPD é um ponto fundamental para a definição do grau de proteção conferido pela LGPD frente a outros países, aumentando a visibilidade internacional do Brasil nos quadros de Estados com as melhores práticas quanto à proteção de dados pessoais.

Sem uma Autoridade devidamente independente e atuante, o Brasil poderá não ser considerado como dotado de grau de proteção adequado e celebrar acordos internacionais de proteção de dados que podem permitir a transferência internacional de dados de maneira menos burocrática, por exemplo.

Nomeação dos cinco membros do Conselho Diretor da ANPD

Em Decreto assinado em 5 de novembro de 2020 e publicado no dia seguinte, em Edição Extra do Diário Oficial da União, foram indicados os 5 (cinco) membros do Conselho Diretor da Autoridade Nacional de Proteção de Dados (ANPD).

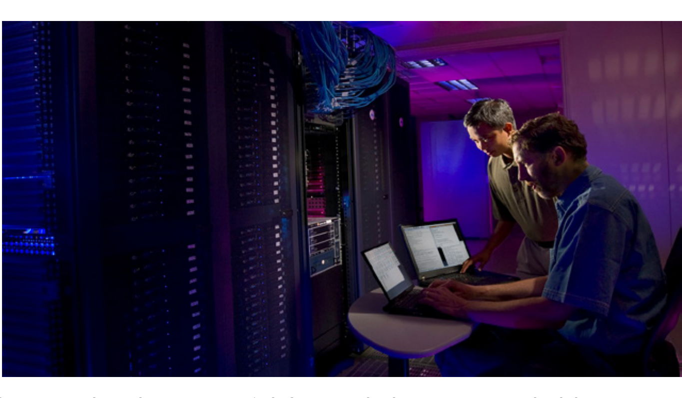
Para o cargo de diretor-presidente do Conselho Diretor da ANPD, foi nomeado Waldemar Gonçalves Ortunho Junior, atual presidente da Telebras, para mandato de 6 (seis) anos. Para os cargos de diretores e diretoras do Conselho Diretor foram nomeados: Arthur Pereira Sabbat, diretor do Departamento de Segurança da Informação do GSI, para mandato de 5 (cinco) anos; Joacil Basilio Rael, militar da reserva e engenheiro da computação, para mandato de 4 (quatro) anos; Nairane Farias Rabelo Leitão, advogada e única representante do setor privado, para mandato de 3 (três) anos; e Miriam Wimmer, diretora de Serviços de Telecomunicações no Ministério das Comunicações, para mandato de 2 (dois) anos.

Segundo o artigo 55-E da Lei Geral de Proteção de Dados, os membros do Conselho Diretor somente perderão seus cargos nas seguintes hipóteses: renúncia; condenação judicial transitada em julgado; ou pena de demissão decorrente de processo administrativo disciplinar, instaurado pelo ministro de Estado Chefe da Casa Civil da Presidência da República e conduzido por comissão especial constituída por servidores públicos federais estáveis. O presidente da República poderá determinar ainda o afastamento preventivo, quando recomendado pela comissão especial, bem como proferir o julgamento.

O Conselho Diretor fica responsável por dispor sobre o regimento interno da ANPD e por indicar os ocupantes dos cargos em comissão e das funções de confiança da ANPD, os quais serão nomeados ou designados pelo diretor-presidente.

Orientações Gerais

As figuras do controlador e do operador na LGPD e as orientações do GDPR



Segundo a Lei Geral de Proteção de Dados, controlador é a pessoa natural ou jurídica, de direito público ou privado, que toma as decisões referentes ao tratamento de dados pessoais, enquanto o operador, também pessoa natural ou jurídica de direito público ou privado, é aquele que realiza o tratamento de dados pessoais em nome do controlador.

Chamados de "agentes de tratamento", a LGPD estabelece a hierarquia e responsabilidade desses agentes, de modo que o operador deverá realizar o tratamento segundo as instruções fornecidas pelo controlador, que devem observar a legislação e eventuais outras normas sobre proteção de dados.

A LGPD estabelece a responsabilidade dos agentes de tratamento de acordo com a ocorrência de danos causados durante o tratamento dos dados, sejam estes danos de ordem patrimonial ou moral, individuais ou coletivos. Apesar da limitação das atividades dos operadores, destaca-se que estes responderão solidariamente pelos danos causados pelas atividades de tratamento realizadas que não tenham observado as orientações fornecidas pelos controladores.

Além disso, de acordo com o princípio da responsabilização e prestação de contas, os agentes de tratamento também são responsáveis pelo cumprimento das demais disposições da LGPD, devendo inclusive implementar medidas adequadas e eficazes para prevenir a ocorrência de incidentes relacionados a dados pessoais, incluindo medidas técnicas e organizacionais.

Segundo o entendimento do Comitê Europeu para a Proteção de Dados (EDPB), que se alinha com as disposições da LGPD, os conceitos de "controlador" e de "operador" devem ser vistos de forma funcional, pois buscam estabelecer as responsabilidades de acordo com os papéis reais de cada um. Isso significa dizer que a qualificação de um agente como controlador ou processador de dados deve ser determinada pelas atividades de fato desenvolvidas, em uma situação concreta, para que a correta responsabilização por eventuais danos causados seja estabelecida.

Avanços Normativos

No processo de definição do Encarregado no Poder Público, o que deve ser levado em consideração?

Muito se discute sobre qual o perfil do profissional indicado para assumir a função de Encarregado (ou "DPO") de cada empresa que trata dados pessoais em sua operação. Reconhecendo que a Administração Pública também trata dados pessoais, a definição de quem serão os encarregados de sua estrutura também merece atenção, em especial considerando que estes indivíduos serão os responsáveis por atuar enquanto ponte de comunicação não apenas entre o governo e a ANPD, mas ainda entre o governo e os titulares dos dados processados em suas atividades.

É diante desse contexto que, em 22 de outubro de 2020, a Secretaria Especial de Desburocratização, Gestão e Governo Digital do Ministério da Economia publicou 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). Como reflexo da relevância da matéria, esta etapa no processo de adequação dos órgãos do SISP à LGPD deve ser concluída em até 30 dias contados da data de vigência da Instrução.

A IN nº 100/2020 prevê ainda a necessidade de qualificação para os encarregados, o que inclui (i) ter "experiência na análise e elaboração de respostas de pedidos de acesso à informação demandados pelo Serviço de Informação ao Cidadão e/ou pela Ouvidoria" e (ii) possuir "conclusão dos cursos de Proteção de Dados no Setor Público e Governança de Dados ou equivalente". Adicionalmente, é apresentada a necessidade de que o indicado (iii) possua "conhecimentos multidisciplinares essenciais a sua atribuição, incluindo as áreas de gestão, segurança da informação, gestão de riscos, tecnologia da informação, proteção da privacidade e governança de dados", o que ganha relevância na medida em que compete ao encarregado, ainda, orientar os colaboradores do agente de tratamento sobre quais as melhores práticas de proteção de dados em sua operação.

Nesse sentido, a IN nº 100/2020 apresenta avanços ao impulsionar a indicação de DPOs em órgãos específicos da Administração Pública e ao estabelecer diretrizes para a seleção de encarregados, que, resguardadas as particularidades de cada setor, podem ser observadas também no setor privado, já que indicam uma série de competências específicas que otimizam o exercício das funções de DPO conforme suas atribuições legais.

Anteprojeto da "LGPD - Penal"

A Comissão de Juristas instituída por Ato do Presidente da Câmara dos Deputados em 26 de novembro de 2019 elaborou o Anteprojeto de Lei de Proteção de Dados para segurança pública e persecução penal ("LGPD – Penal"), destinada a regular o tratamento de dados no âmbito da segurança pública e de atividades de persecução e repressão de infrações penais.

Na exposição de motivos do anteprojeto, foi ressaltada a necessidade de edição de lei específica para o tema de tratamento de dados realizado para fins de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais, assim como consta no parágrafo 1º do art. 4º da LGPD. Segundo a Comissão, o Anteprojeto busca estabelecer diretrizes para operações de tratamento de dados pessoais nas atividades de segurança pública e de persecução criminal, a fim de assegurar a proteção de dados e do próprio titular contra mau uso e abusos, e, ao mesmo tempo, garantir o cumprimento dos deveres do Estado na prevenção e na repressão de ilícitos criminais e proteção da ordem pública.

O anteprojeto apresenta princípios tanto de matéria de proteção de dados quanto de matéria penal, como presunção de inocência e garantia do devido processo legal, da ampla defesa, do contraditório, da motivação e da reserva legal. Estabelece ainda a aplicabilidade da Lei a qualquer operação de tratamento realizada por autoridades competentes em atividades de segurança pública e de persecução penal, com exceção ao tratamento de dados pessoais realizado para fins exclusivos de defesa nacional e segurança do Estado.

O anteprojeto traz novos conceitos como dado pessoal sigiloso para definir dado pessoal protegido por sigilo constitucional ou legal, bem como definição específica para a figura do controlador, que seria a autoridade competente responsável pelas decisões referentes ao tratamento de dados pessoais. Autoridade competente, por sua vez, seria a autoridade pública, órgão ou entidade do Poder Público responsável pela prevenção, detecção, investigação ou repressão de atos infracionais e infrações penais ou execução de sanções penais. Outros novos conceitos trazidos também pelo anteprojeto são atividade de segurança pública, atividade de persecução penal, tecnologia de monitoramento e registros criminais.

O anteprojeto estabelece uma classificação para os titulares de dados nas seguintes categorias: pessoas em relação às quais existem indícios suficientes de que cometeram uma infração penal; pessoas em relação às quais existem indícios suficientes de que estão prestes a cometer uma infração penal; pessoas processadas pela prática de infração penal; pessoas condenadas definitivamente pela prática de infração penal; vítimas de uma infração penal ou pessoas em relação às quais certos fatos indicam que podem ser vítimas de uma infração penal; e outras pessoas, tais como testemunhas, pessoas que possam fornecer informações, ou contatos ou associados das pessoas mencionadas anteriormente.

Novas bases legais para o tratamento de dados foram prescritas como cumprimento de atribuição legal de autoridade competente, na persecução do interesse público; execução de políticas públicas; e proteção da vida ou da incolumidade física do titular ou de terceiro, contra perigo concreto e iminente. Por fim, entre outras disposições, o anteprojeto prevê a criação de um tipo penal, o qual tipifica a transmissão ilegal de dados, realizada para obter vantagem indevida ou causar prejuízos a outrem, com pena de reclusão, de 1 a 4 anos, e multa.

Poder Judiciário

STJ sofre ataque de hackers

No dia 04/11/2020, o Superior Tribunal de Justiça informou que sofreu um ataque de hackers no dia 03/11/2020, quando foi detectado um vírus circulando na rede de informática do Tribunal, que deixou a sua base de dados inacessível, impedindo a tramitação usual de processos, além do acesso interno a e-mails.

Em razão do incidente, o Tribunal suspendeu todas as sessões de julgamento, bem como os prazos processuais até o dia 09/11/2020, por meio da Resolução STJ/GP nº 25, de 04/11/2020.

Além disso, a Presidência do Tribunal informou ter solicitado que a Polícia Federal procedesse às devidas investigações, por meio de notícia-crime. Foi determinada a instauração de inquérito pelo ministro da Justiça, André Mendonça.

O STJ esclareceu que, apesar do ataque hacker ter bloqueado o acesso a dados por meio de criptografia, os dados estariam preservados nos sistemas de backup do tribunal, de modo que as informações referentes a processos judiciais, contas de e-mails e contratos administrativos permaneceram íntegras e inalteradas.

Os sistemas de informática do STJ foram restabelecidos no dia 09/11 e a partir do dia 10/11/2020 as atividades do Tribunal começaram a ser retomadas, incluindo o acesso ao site e serviços de consulta processual. Os prazos processuais também voltaram a correr no dia 10/11/2020.

Além do STJ, outros órgãos também foram atingidos por ataque de hackers: o Ministério da Saúde, a Secretaria de Economia do Distrito Federal e o governo do Distrito Federal.

Isso demonstra que o caminho da adequação à LGPD precisa ser tomado de forma rápida pelos órgãos públicos, que necessitam dar mais importância às questões de segurança cibernética e proteção de dados, a fim de evitar novos ataques e vazamento de dados.

CNJ anuncia criação de comitê cibernético

O ministro Luiz Fux, presidente do CNJ, anunciou a criação do Comitê de Segurança Cibernética do Poder Judiciário, por meio da Portaria CNJ nº 242/2020, publicada em 11/11/2020.

A criação desse comitê se dá em decorrência do ataque hacker sofrido pelo STJ e tem como objetivo reforçar a segurança dos sistemas digitais dos tribunais e demais órgãos jurisdicionais, bem como garantir que o Poder Judiciário atenda a população com segurança e responsabilidade por meio das soluções digitais, conforme declaração do ministro Luis Fux.

De acordo com a Portaria CNJ nº 242/2020, o Comitê de Segurança Cibernética do Poder Judiciário será composto por dois representantes do CNJ, além de um representante indicado pelo STF, STJ, TSE, TST, CJF e STM, bem como dois representantes dos Tribunais de Justiça Estaduais. Estes representantes deverão ter conhecimento técnico na área de segurança cibernética.

Além disso, o comitê poderá convidar representantes de órgãos de segurança pública, das Forças Armadas e especialistas técnicos de outros órgãos públicos ou privados para subsidiar os respectivos trabalhos.

Quanto aos trabalhos a serem exercidos pelo comitê, a citada Portaria estipula que devem ser entregues nos próximos meses à Presidência do CNJ o Protocolo de Prevenção e Protocolo de Gerenciamento de Crises para o enfrentamento de ilícitos cibernéticos no Judiciário, bem como o Protocolo de Investigação para ilícitos cibernéticos que possam afetar as atividades dos órgãos judiciais, além de minuta de Estratégia da Segurança Cibernética e da Informação do Judiciário.

Outra atribuição estabelecida pela Portaria ao comitê consiste na proposição de norma para a criação, a ativação e o efetivo funcionamento do Centro de Tratamento de Incidentes de Segurança Cibernética (CTISC) do CNJ, que funcionará como canal oficial para orquestração e divulgação de ações preventivas e corretivas, em caso de ameaças ou de ataques cibernéticos.

A criação do Comitê de Segurança Cibernética do Poder Judiciário e a definição dos trabalhos a ele atribuídos por meio da Portaria CNJ nº 242/2020 demonstram que o Poder Judiciário brasileiro tomou uma atitude rápida em resposta ao ataque hacker recentemente sofrido pelo STJ, e que está em busca de garantir aos jurisdicionados as melhores medidas de segurança para evitar que um novo incidente de segurança cibernética ocorra novamente.

CNJ cria grupo de trabalho para adequar o Judiciário à LGPD

O CNJ publicou no dia 16/10/2020 a Portaria nº 212/2020, que designou os membros do grupo de trabalho que irá elaborar estudos e propostas para adequar os tribunais brasileiros à LGPD. O grupo será coordenado por Henrique de Almeida Ávila, conselheiro do CNJ, e terá outros 15 integrantes, dentre magistrados e renomados advogados e professores atuantes na pesquisa do tema de proteção de dados.

Entre os objetivos do grupo de trabalho está a proposição de audiência e consultas públicas, palestras e seminários com representantes de órgãos públicos e de entidades da sociedade civil, além de especialistas no assunto.

Assim, na linha do que estipulado na Recomendação CNJ nº 73/2020, o órgão demonstra, mais uma vez, a preocupação do Poder Judiciário para com a tomada de medidas efetivas para implementação da LGPD.

TJSC lança capacitação para magistrados sobre LGPD

Demonstrando a atuação efetiva dos tribunais estaduais para com a implementação da LGPD, a Academia Judicial do Poder Judiciário do Estado de Santa Catarina, juntamente com o Comitê Gestor de Proteção de Dados Pessoais (CGPDP), órgão vinculado à Presidência do TJSC, realizará sua primeira capacitação para magistrados sobre a Lei Geral de Proteção de Dados Pessoais, que acontecerá por meio de plataforma online, nos meses de novembro e dezembro.

STF publica acórdão referendando a decisão liminar que suspendeu os efeitos da Medida Provisória nº 954/2020

Como um relevante e inédito precedente para o tema da proteção de dados, foi publicado no Diário Oficial no dia 12 de novembro o acórdão relativo ao julgamento da ADI nº 6387 pelo STF realizado em plenária em 07 de maio de 2020, que suspendeu a eficácia da Medida Provisória nº 954/2020. Tal MP, emitida pelo Governo Federal, dispõe sobre o compartilhamento de dados por empresas de telecomunicações com a Fundação Instituto Brasileiro de Geografia e Estatística (IBGE), para fins de suporte à produção estatística oficial durante a situação de emergência de saúde pública.

Sob a relatoria da ministra Rosa Weber, a medida cautelar foi referendada pelos demais ministros do Supremo Tribunal Federal, restando vencido apenas o ministro Marco Aurélio, abarcando, portanto, as demais 4 ADIs também ajuizadas em face da referida MP (ADIs nºs 6388, 6389, 6390 e 6393).

Privilegiando a proteção constitucional da liberdade individual (art. 5º, caput), da privacidade e do livre desenvolvimento da personalidade (art. 5º, X e XII) os principais fundamentos que justificaram a concessão da medida foram (i) a necessidade de proteção das informações previstas na MP, já que relacionadas à identificação – efetiva ou potencial – de pessoa natural e que configuram dados pessoais; (ii) o respeito à privacidade e à autodeterminação informativa – já positivados no art. 2º, I e II, da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais); e (iii) a ausência de delimitação do objeto da estatística a ser produzida, tampouco a finalidade específica e sua amplitude.

Evidenciou-se, ainda, a ausência de demonstração, pela MP, do interesse público legítimo no compartilhamento dos dados pessoais dos usuários dos serviços de telefonia, considerados a necessidade, a adequação e a proporcionalidade. Ainda, considerou-se que a MP não apresentou mecanismo técnico ou administrativo apto a proteger os dados pessoais de acessos não autorizados, vazamentos acidentais ou utilização indevida, seja na sua transmissão, seja no seu tratamento.

Desse modo, embasado no diálogo das fontes com as demais jurisdições relativas à proteção de dados, o STF debateu o tema como direito fundamental. A relevância de tal precedente se mostra não somente em razão da gravidade das medidas estabelecidas pela MP – e agora afastadas – mas porque estamos diante de importante julgamento proferido ainda antes da vigência das previsões contidas na LGPD e ainda ausente a ANPD, mas que demonstram como a discussão foi levada ao Poder Judiciário e com a imediata aplicação de seus princípios (em especial adequação, proporcionalidade, finalidade, autodeterminação informativa), o que será uma constante a ser observada adiante.

Proteção ao Consumidor

PROCON-SP notifica empresas sobre cadastros e contratações sem autorização de usuários

O lançamento do PIX como meio de pagamentos chamou a atenção do público e da imprensa e trouxe atenção dos órgãos de defesa do consumidor.

Especificamente quanto a proteção de dados pessoais, o PROCON-SP recentemente recebeu denúncias de consumidores que teriam tido cadastrados seus dados sem permissão. Por isso, notificou as fintechs Mercado Pago e Nubank a esclarecerem a esse respeito.

As empresas negaram irregularidades em sua manifestação e esclareceram que os cadastros teriam sido feitos com a autorização dos usuários.

Noticiada a notificação do PROCON-SP, três entidades que representam o setor das fintechs fizeram pronunciamento conjunto esclarecendo que 0,01% das chaves cadastradas pelas principais empresas de tecnologia financeira teriam tido algum problema.

Na mesma linha sobre suposto uso desautorizado de informações de consumidores, o Banco C6 Consignado concedeu crédito consignado a aposentados sem sua autorização.

O PROCON-SP notificou o C6 Consignado após serem registradas 149 reclamações em apenas um mês referentes a empréstimos consignados não contratados pelos consumidores.

O diretor-executivo do PROCON-SP, Fernando Capez, ao se manifestar, disse que a atuação do banco seria ilegal, tratando-se de infração "gravíssima", na medida em que faria mau uso de dados pessoais de aposentados em poder do banco, em "grave violação ao sigilo de dados", sendo que esses dados sequer deveriam estar em poder do Banco C6, uma vez que oriundos do INSS.

Sobre a mesma suposta prática do Banco C6 Consignados, o PROCON de Patos de Minas-MG solicitou ao Ministério Público Federal uma investigação a respeito da conduta.

PROCON-SP notifica Enel por vazamento de dados

Tendo sido noticiado o suposto vazamento de dados pessoais de grande número de clientes da Enel residentes em Osasco (região metropolitana de São Paulo), o PROCON-SP notificou a Enel para prestar esclarecimentos a respeito.

O prazo para a empresa se manifestar é de 72 horas e, a requerimento do PROCON-SP, a Enel deverá mostrar as medidas de segurança que adota para proteger o sigilo dos dados pessoais de seus clientes, esclarecer se houve o treinamento de seus funcionários a respeito da aplicação da Lei Geral de Proteção de Dados, e explicar por que não houve a criptografia de dados como CPF e número de telefone de seus consumidores na coleta e processo de tratamento dos dados. O órgão também requisitou a apresentação das medidas tomadas para resolução de possíveis danos decorrentes do incidente, declaração da equipe dedicada à resposta e relatório de impacto.

IDEC aponta preocupação com informação de pacientes em marketplace de empresa

Com a vigência da LGPD, as entidades de defesa do consumidor aceleraram os seus questionamentos ao tratamento de dados adotado em diversas empresas.

No mês de outubro de 2020, o Instituto de Defesa do Consumidor (IDEC) enviou questionamentos a empresa do ramo da saúde a respeito de seu novo marketplace, que reúne prestadores de serviços, armazena prontuários, além de conter outras funções como venda de medicamentos, alimentos saudáveis e uso de algoritmos para medicina preventiva.

O IDEC questionou sobre a coleta das informações dos pacientes e o compartilhamento de dados com farmacêuticas e planos de saúde, tendo a empresa respondido que segue as disposições da LGPD, além de manter um rigoroso sigilo médico.

Vale lembrar que o IDEC também já havia feito questionamentos a uma empresa do ramo do vestuário, em razão do uso de tecnologia de reconhecimento facial sem avisos suficientes ao cliente, sendo que, em razão da denúncia do Instituto, a SENACON aplicou multa à empresa.

Sendo assim, mostra-se relevante a atuação das entidades de defesa do consumidor, lado a lado aos órgãos públicos, para verificação da conformidade de empresas com a LGPD.

SENACON na mídia - Intersecção entre a proteção de dados e a proteção ao consumidor

Em recente entrevista concedida à Lex Marketing (MLex), a secretária nacional do Consumidor, Juliana Domingues, declarou que, em razão do início da vigência da LGPD, a expectativa é por um aumento no número de reclamações dos consumidores relacionadas aos seus direitos como titulares de dados pessoais.

No entendimento da secretária, tal aumento se dará, pois os consumidores estarão mais informados sobre os valores e princípios previstos na lei, e cada vez mais atentos ao uso de seus dados sem o devido consentimento.

Neste cenário, a ANPD – cujos membros foram nomeados e divulgados no Diário Oficial da União no último dia 06 de novembro – figurará como a Autoridade responsável por trilhar as diretrizes para interpretação e implementação da LGPD, bem como conceder um prazo para que sejam implementados mecanismos de proteção de dados pessoais por todos os integrantes do cenário brasileiro, bem como o desenvolvimento da própria cultura de respeito à lei em nosso país.

Apesar disso, a secretária entende que as empresas de grande porte já estão muito bem preparadas para lidar com os desafios relativos à proteção de dados, na medida em que as regras previstas no Código de Defesa do Consumidor (CDC) e também no Marco Civil da Internet já dispunham sobre o necessário cuidado com o tratamento de dados pessoais. Nesse sentido, a secretária entende como extremamente necessário o diálogo entre as autoridades brasileiras no tocante ao tema da proteção de dados, compatibilizando as atuações da ANPD, SENACON e Ministérios Públicos.

A própria SENACON, embasada nas previsões e sanções do CDC, já tem ativamente atuado com especial atenção às condutas praticadas por plataformas digitais, tendo em vista um aumento significativo de reclamações dos consumidores durante o período de pandemia da COVID-19, buscando ajustar em nosso país um ambiente digital mais seguro.

Ainda, a fim de ampliar a atuação e incessante promoção da proteção aos dados pessoais, a SENACON firmou acordo com o FTC (US Federal Trade Commission) para ingressar na plataforma denominada "*Econsumer*", onde será possível fazer o reporte de fraudes aos direitos dos consumidores em diferentes jurisdições. A secretária entende que esta é uma maneira de monitorar e identificar fraudes transnacionais, em especial em um cenário cada vez maior de utilização de algoritmos e publicidade automatizadas por empresas com atuação internacional. Nesse mesmo sentido, a SENACON também se juntou recentemente ao comitê de proteção ao consumidor da OCDE com o objetivo de discutir as práticas de marketing digital e o tema de proteção de dados.

É evidente, portanto, a constante sinalização da SENACON quanto ao seu interesse de atuar ativamente na proteção de dados, embasada não somente nas regras contidas na LGPD e que serão foco da ANPD, mas sim nas amplas regras de proteção ao consumidor que, há muito, garantem o necessário cuidado com o tratamento de dados e devem ser tidas como o foco das práticas e novas políticas implementadas pelas empresas que assim atuarem.

Ministério Público

Nova página no site do MPDFT reúne informações sobre a LGPD

O Ministério Público do Distrito Federal e Territórios (MPDFT) lançou, em 23/10/2020, uma nova página em seu site, com o objetivo de prestar informações à sociedade sobre **(i)** como a instituição atua em atenção às leis vigentes (com destaque para a LGPD), na proteção dos dados pessoais que trata no desempenho de suas funções; assim como atua **(ii)** para proteger e ver resguardados nos termos da legislação vigente (com destaque para a LGPD) os dados pessoais dos brasileiros. Referida página, recém-lançada pelo MPDFT, pode ser acessada no seguinte endereço: https://www.mpdft.mp.br/portal/index.php/lgpd.

Na seção **(i)** de tal página, o visitante encontra informações sobre quais ações são adotadas pelo MPDFT para atender ao disposto na legislação vigente acerca da necessária proteção aos dados pessoais que são tratados no exercício das funções institucionais do Ministério Público. Nessa mesma seção **(i)**, o usuário encontra descrição de quais são os seus direitos, acerca de seus dados pessoais que venham a ser ou que estejam sendo tratados pelo MPDFT.

Por sua vez, a seção **(ii)** da página detalha quais são as ações realizadas pela Unidade Especial de Proteção de Dados e Inteligência Artificial (ESPEC) do MPDFT, em atuação visando à proteção dos dados pessoais de brasileiros, dentre as quais: instauração de procedimentos preparatórios, de inquéritos civis públicos e de procedimentos administrativos; propositura de ações judiciais; promoção, entre a população, empresas e órgãos públicos, do conhecimento acerca das normas e das políticas públicas sobre a proteção de dados pessoais, privacidade e medidas de segurança; promoção de estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade; promoção de ações de cooperação com autoridades de proteção de dados pessoais de outros países, inclusive para receber comunicações sobre a ocorrência de qualquer incidente de segurança que possa acarretar em risco ou prejuízo relevante aos titulares dos dados; e até mesmo sugestão de diretrizes para uma Política Nacional de Proteção dos Dados Pessoais e Privacidade.

Em referida seção **(ii)** da página, o MPDFT destaca que, somente entre 2019 e 2020, já adotou cerca de 50 (cinquenta) medidas visando à proteção dos dados pessoais de brasileiros, via as linhas de atuação acima destacadas.

MPDFT obtém tutela de urgência com base na LGPD, para impedir a comercialização de dados pessoais via anúncios postados por usuário na plataforma Mercado Livre

Em 14/10/2020, o MPDFT ajuizou uma ação civil pública a fim de que cessasse alegada comercialização de dados pessoais, realizada via anúncios postados por um usuário de internet, na plataforma do Mercado Livre (autos nº 0733785-39.2020.8.07.0001). Referida comercialização de dados pessoais alegadamente abrangia informações de nome, número de cadastro de CPF, número de telefone fixo e de celular, bem como informações de endereço.

Em decisão proferida em 15/10/2020, o magistrado deferiu a tutela de urgência pleiteada, para que o autor dos anúncios objeto da ação suspendesse a prática de venda de dados pessoais; tendo sido também determinada a expedição de ofício ao Mercado Livre para que procedesse à indisponibilização de tais anúncios, bem como ao fornecimento dos dados cadastrais acerca do usuário autor destes. O Mercado Livre já apresentou resposta a ofício, cumprindo a ordem de indisponibilização de anúncios e de fornecimento dos dados cadastrais acerca do usuário autor destes.

Decisões Internacionais

A maior penalidade aplicada pela Autoridade Inglesa até o momento: o entendimento de ineficiência da British Airways na prevenção e resolução de incidentes de segurança

Em 16 de outubro de 2020, a Autoridade de Proteção de Dados Inglesa (o "Information Comissioner's Office" ou "ICO"), com fundamento no GDPR, aplicou multa no valor de 20 milhões de libras à companhia aérea British Airways pela não adoção medidas de segurança aptas a identificar e resolver falhas de segurança em ataque cibernético ocorrido em 2018. Trata-se da maior multa aplicada pelo ICO desde que o GDPR entrou em vigor.

Na ocasião, a base de dados da British Airways foi alvo de um incidente de segurança cibernético que resultou no vazamento dos dados de aproximadamente 430 mil funcionários e clientes no decorrer de duas semanas (desde dados cadastrais até suas informações financeiras), o que foi identificado pela empresa apenas dois meses depois do ocorrido. Segundo o ICO, a companhia aérea tratava dados sem a adoção das medidas de segurança adequadas para resguardá-los (uma vez que não limitava o acesso aos dados tratados em suas atividades ou realizavas testes rigorosos de simulação de ciberataques), o que, por si só, já configura violação às garantias estabelecidas no GDPR. Vale ressaltar que além da gravidade do incidente frente ao volume de titulares afetados, a aplicação da alta multa pela Autoridade considerou ainda enquanto agravante a postura omissa da British Airways frente ao ocorrido por tamanho período.

Em consonância com a legislação brasileira, a aplicação de multa com valores na mesma faixa e com fundamentos em sintonia com aqueles apresentados pelo ICO poderia ser uma realidade no Brasil. Segundo o art. 46 da LGPD, os agentes de tratamento de dados "devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais" contra incidentes de segurança, como estes que incluem qualquer acesso não autorizado a bases de dados (como ocorrido com a British Airways) ou ainda situações acidentais ou ilícitas que resultem, por exemplo, em perda, comunicação ou alteração de dados pessoais. Na hipótese de concretização de um incidente, entretanto, os agentes também ficam sujeitos à aplicação de sanções administrativas pela Autoridade Nacional de Proteção de Dados (ANPD), que pode aplicar não apenas advertências ou ordens de suspensão do banco de dados afetado, mas ainda multas de até 50 milhões de reais pela infração (em paralelo com o aplicado pelo ICO).

Fonte: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-fines-british-airways-20m-for-data-breach-affecting-more-than-400-000-customers/

Cooperação entre as autoridades europeias

Tanto no caso da British Airways como em outros casos relevantes de apuração de incidentes envolvendo dados pessoais e a aplicação de sanções, é possível verificar forte cooperação entre as autoridades de proteção de dados europeias. No caso da British Airways, embora a Information Commissioner's Officer (ICO) tenha coordenado as investigações e imposto as sanções no caso, os projetos de decisões foram enviados a outras autoridades de proteção de dados europeias, como a Commission Nationale de l'Informatique et des Libertés (CNIL), autoridade francesa sobre o tema.

Esse mecanismo de cooperação está previsto no Regulamento Geral de Proteção de Dados da União Europeia (GDPR) e busca harmonizar as decisões referentes aos tratamentos de dados transfronteiriços. Referido como "guichet unique" pela autoridade francesa, o mecanismo conta com três pontos principais: (i) se destina apenas a empresas situadas na União Europeia, que operam tratamentos de dados em mais de um país; (ii) a decisão deve contar com apenas um interlocutor principal, a autoridade nacional de proteção de dados do país ou do país onde se encontra a sede da empresa, o qual será responsável por tomar a decisão em conjunto com as demais autoridades envolvidas no tratamento transfronteiriço; (iii) busca estabelecer uma só decisão válida em todo o território da União Europeia.

Em matéria de cooperação, o cenário brasileiro da LGPD atribui à ANPD a promoção de ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transnacional, razão que também corrobora a importância de que a ANPD tenha autonomia técnica e decisória no decorrer de suas atividades.

IMAGENS: ALTUM CODE, CLINT PATTERSON, DAN ARSKY, DAVID DVORACEK, MARCOS OLIVEIRA (AGÊNCIA SENADO), NATIONAL CANCER INSTITUTE, SAMSUNG, SCIENCE IN HD.

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

Este material não pode ser reproduzido integralmente ou parcialmente sem consentimento e autorização prévios de TozziniFreire Advogados.