TF cybernews
6ª edição | 2021
TOZZINIFREIRE ADVOGADOS

Realidade Brasileira

ANPD divulga o Planejamento Estratégico para suas atividades de 2021 a 2023

A Autoridade Nacional de Proteção de Dados (ANPD) publicou o seu Planejamento Estratégico para os anos de 2021-2023, o que delimita com maior clareza os macro-objetivos que norteiam suas atividades, bem como os prazos para a implementação dessas metas.

O Planejamento estabelece ainda missão, a visão e os valores da ANPD. Nesse sentido, a Autoridade vislumbra seu objetivo de "zelar pela proteção dos dados pessoais" (sua missão), buscando "tornar-se órgão de referência nacional e internacional com relação à Proteção de Dados Pessoais" (sua visão) e atuando, para tanto, com "ética, transparência, integridade, imparcialidade, eficácia e responsabilidade" (seus valores).

Sob esse norte, os três macro-objetivos estratégicos que a ANPD almeja alcançar nos próximos anos são:

i. A promoção do fortalecimento da cultura de proteção de dados pessoais, o que reúne ações estratégicas voltadas à prevenção e à detecção de infrações à LGPD, assim como ações dirigidas à capacitação e à orientação dos agentes de tratamento e da sociedade quanto às normas de proteção de dados pessoais (promovendo, então, um diálogo mais ativo com instituições privadas e governamentais);
ii. O estabelecimento do ambiente normativo eficaz para a proteção de dados pessoais, o que diz respeito ao estabelecimento de prioridades em sua agenda regulatória, à criação e aprovação dos temas regulatórios e o estabelecimento de procedimentos e mecanismos céleres para o tratamento de incidentes e de reclamações; e
iii. O aprimoramento das condições para o cumprimento das competências legais, o que reúne, por sua vez, as ações voltadas para a garantia de condições físicas, orçamentárias e de recursos humanos adequadas e suficientes para garantir o bom funcionamento da ANPD.

Diante desse panorama, o Planejamento dá publicidade às iniciativas e organização da Autoridade, contribuindo para a criação de um ambiente de Proteção de Dados com maior segurança jurídica, transparência e previsibilidade com relação aos diversos pontos da LGPD pendentes de regulação específica.

Vale ressaltar que a ANPD tem papel central na estruturação da cultura de proteção de dados no Brasil, através da elaboração de diretrizes, parâmetros e orientações, além de ser uma instituição fundamental para posicionar o país no contexto global de proteção de dados, cada vez mais competitivo.

Em atenção à sua agenda regulatória, ANPD inicia em janeiro a tomada de subsídios sobre microempresas e sobre a notificação de incidentes de segurança

Em 29 de janeiro deste ano, a Autoridade Nacional de Proteção de Dados (ANPD) deu início à tomada de subsídios por parte da sociedade civil para a regulamentação das especificidades da Lei Geral de Proteção de Dados (LGPD) que lhe cabem.

Em específico, nesta ocasião, a ANPD busca contribuições para o desenho da "regulamentação aplicável para microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação e pessoas físicas que tratam dados pessoais com fins econômicos".

Entre os pontos objeto de discussão nesta consulta, são levantadas algumas questões específicas pela ANPD para o recebimento de considerações a respeito. Nesse sentido a Autoridade busca contribuições relacionadas a pontos tais como os critérios que deveriam ser considerados na definição de agentes de tratamento de dados de pequeno porte, a definição dos impactos da nomeação de um encarregado de dados aos agentes de pequeno porte, e ainda dos impactos da implementação do tratamento de dados em conformidade com a LGPD aos agentes de pequeno porte.

Nesse processo, a Autoridade recebeu contribuições até 1º de março de 2021, período em que a ANPD realizou reuniões com agentes públicos e privados envolvidos no tema.

Vale ressaltar que a regulamentação diferenciada para microempresas e empresas de pequeno porte é um dos temas objeto da primeira fase da Agenda Regulatória da ANPD para o biênio 2021-2022 (publicada em 28 de janeiro, no âmbito da Portaria nº 11/2021). Como resultado, a tomada de subsídios sobre o tema (iniciada em apenas 1 dia após a publicação da referida agenda), denota a prontidão e o compromisso por parte da Autoridade ao dar os primeiros passos rumo à implementação do seu cronograma de atividades.

Em complemento à tomada de subsídios sobre microempresas, ANPD iniciou também um processo de tomada de subsídios sobre a notificação de incidentes de segurança nos termos do Art. 48 da LGPD. As contribuições devem seguir um modelo divulgado no site da ANPD e podem ser enviadas de 22/02/2021 até 24/03/2021 (acesse aqui).

A ANPD já disponibilizou um formulário de comunicação de incidente de segurança de dados pessoais, bem como um documento de orientação em caso de incidentes, que servirão como guias para os controladores de dados enquanto não houver a regulamentação específica da autoridade sobre os temas (acesse aqui).

Essas iniciativas estão alinhadas com a expectativa regulatória da ANPD, que previa o início da regulamentação de incidentes de segurança de dados pessoais (em especial a comunicação de incidentes e especificação do prazo de notificação) em sua Agenda Regulatória ainda em 2021.

ANPD convoca candidaturas para a formação do Conselho Nacional de Proteção de Dados

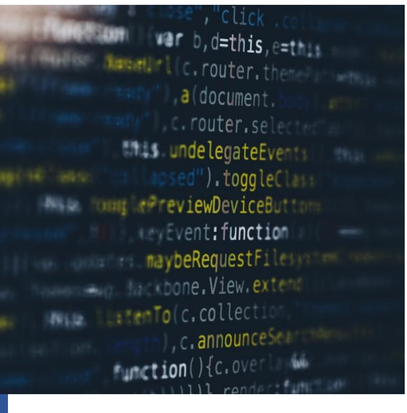
Foram publicados, no Diário Oficial da União, no início deste mês, os Editais para formação de lista tríplice, pela Autoridade Nacional de Proteção de Dados (ANPD), para a composição do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade (CNPD) que, formado por 23 (vinte e três) membros titulares e reunindo-se ordinariamente 3 (três) vezes ao ano, terá como principais atribuições: (i) propor diretrizes estratégicas e fornecer subsídios para a elaboração da Política Nacional de Proteção de Dados Pessoais, (ii) elaborar relatórios anuais de avaliação da execução das ações da Política Nacional, (iii) sugerir ações a serem realizadas pela ANPD, (iv) elaborar estudos e realizar debates e audiências públicas sobre a proteção de dados pessoais e da privacidade, e (v) disseminar o conhecimento sobre a proteção de dados e da privacidade à população.

Por meio dos editais, a ANPD convocou as organizações civis com atuação em proteção de dados pessoais, as instituições científicas, tecnológicas e de inovação e as Confederações Sindicais representativas das categorias econômicas do setor produtivo para indicarem um nome, cada, para integrar lista tríplice que preencherá 3 (três) vagas no Conselho.

Por sua vez, as entidades representativas do setor empresarial relacionado à área de tratamento de dados pessoais e as entidades representativas do setor laboral também foram convocadas para indicar um nome, cada, para a formação de lista tríplice para o preenchimento de 2 (duas) vagas no Conselho Nacional.

Cabe ressaltar que a escolha dos nomes para a lista tríplice será realizada através de critérios como a representatividade e a experiência na área de proteção de dados do candidato e que todas as vagas têm mandato de 2 (dois) anos, sendo permitida apenas uma recondução, por igual período.

Poder Judiciário



Instituto Sigilo ajuíza ação civil pública contra Serasa Experian por "megavazamento" de dados

Em que pese ainda estejam em curso as investigações administrativas iniciadas pela SENACON e pelo PROCON-SP acerca da empresa responsável pelo megavazamento de dados que atingiu mais de 220 milhões de brasileiros, o Instituto Brasileiro de Defesa da Proteção de Dados Pessoais Sigilo ("Instituto Sigilo") ajuizou ação civil pública em face da Serasa Experian.

Nela, o Instituto Sigilo acusa a empresa pelo megavazamento de dados, requerendo, no mérito, a condenação da Serasa Experian ao pagamento de danos morais coletivos no valor de R$ 200 milhões, além de indenização no valor de R$ 15 mil para cada um dos titulares de dados afetados pelo vazamento. Além dos pedidos indenizatórios, o Instituto pleiteia, liminarmente, que a empresa comunique individualmente, por carta com aviso de recebimento, todos os titulares afetados pelo vazamento, bem como divulgue quais foram os incidentes de segurança da informação ocorridos e quais providências serão adotadas para (i) retirar os dados vazados da internet; (ii) cessar os prejuízos aos titulares e, ainda, (iii) solucionar os eventuais e futuros riscos aos seus consumidores. Ainda em caráter liminar, requer que seja determinada à União a realização de auditoria sobre o vazamento em questão.

No polo passivo da demanda o Instituto Sigilo também incluiu a União, na figura da ANPD, alegando uma suposta omissão da Autoridade e buscando liminarmente que notifique a Serasa Experian, realize auditoria técnica para constatar a falha de segurança ocorrida no incidente, bem como comunique os titulares dos dados pessoais sobre o vazamento ocorrido.

Após a intimação da União para manifestação, ainda resta pendente a apreciação do pedido de tutela de urgência.

Dados dos 11 ministros do STF são colocados à venda após maior vazamento de dados já registrado no país

Ainda sobre o "megazavamento", constatou-se que os dados de algumas autoridades do país estão à venda na internet, incluindo aqueles referentes aos 11 ministros do STF.

A pedido do jornal "O Estado de S. Paulo", uma empresa de segurança verificou que os dados ofertados pelo responsável pelo vazamento são divididos em 37 categorias, sendo que todos os ministros do STF possuem dados vazados em mais de 20. De acordo com o material publicado, eles estariam sendo vendidos em pacotes a partir de US$ 500,00, sendo que 10 é o limite máximo de categorias de dados que poderiam ser adquiridas de um único CPF.

Ressalta-se que a categoria "básico simples", que inclui CPF, nome completo, sexo, gênero e data de nascimento, foi a única integralmente publicada e que atingiu o maior número de cidadãos, não sendo possível confirmar se os responsáveis pelo vazamento dos dados realmente possuem todas as informações que alegam ofertar.

Após a divulgação da informação, o ministro presidente do STF, Luiz Fux, encaminhou ofícios ao ministro da Justiça, André Mendonça, e ao ministro Alexandre de Moraes, relator do Inquérito nº 4.781 ("Inquérito das Fake News"), solicitando que sejam adotadas providências. Nesse sentido, o ministro Alexandre de Moraes proferiu despacho determinando à Polícia Federal a abertura de inquérito para investigação do episódio, ressaltando que este atinge diretamente a privacidade, intimidade e segurança dos integrantes da Corte. Além disso, no mesmo despacho, requereu que o relatório elaborado pelo perito seja autuado no STF e, por prevenção, o processo também será de relatoria do ministro

Ouvidoria passa a ser encarregada da proteção dos dados pessoais no TSE

No dia 12 de janeiro de 2021, o Tribunal Superior Eleitoral publicou a Portaria nº 14/2021, que instituiu a unidade encarregada pela proteção de dados pessoais no âmbito de atuação do Tribunal. A Ouvidoria do TSE passará a ser o órgão responsável pelo recebimento de reclamações e dúvidas de pessoas que tiveram os seus dados tratados pelo Tribunal.

Segundo o artigo 5º, inciso VIII, da LGPD, o encarregado é aquele indicado para "atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)". Além disso, o artigo 41, § 2º, da mesma Lei estabelece quais são as atividades do encarregado, que deve adotar providências com relação às reclamações recebidas dos titulares e comunicações estabelecidas com a ANPD, bem como orientar os funcionários do órgão no tocante às medidas que devem ser adotadas para a proteção dos dados pessoais. Ressalta-se, no entanto, que conforme previsto no § 3º do referido dispositivo, a ANPD poderá estabelecer normas complementares sobre as atribuições do encarregado.

De acordo com as informações publicadas pelo TSE, as comunicações sobre o tratamento de dados pessoais deverão ser encaminhadas diretamente à Ouvidoria pelos seus canais de comunicação, sendo certo que o atendimento ao público está sendo realizado por meio de ligação telefônica ou pelo preenchimento de um formulário eletrônico, que solicita as seguintes informações: nome, faixa etária, Unidade Federativa e e-mail.

Proteção ao Consumidor

Iniciadas investigações administrativas para identificar a origem de “megavazamento” de dados

Diante do “megavazamento” de dados que revelou informações pessoais como nome, CPF, fotografia, salário, renda, nível de escolaridade, estado civil, score de crédito e endereço de mais de 220 milhões de brasileiros, autoridades administrativas ligadas à defesa do consumidor iniciaram investigações com o propósito de identificar a fonte do incidente:

- A SENACON (Secretaria Nacional do Consumidor) notificou a Serasa Experian, buscando o oferecimento de explicações quanto ao possível envolvimento da empresa no vazamento de dados e em relação a quais dados teriam sido vazados, a quem e por quanto tempo, bem como se a empresa tem adotado medidas para melhorar a segurança da privacidade dos titulares dos dados;
- O PROCON-SP também notificou a Serasa Experian, solicitando esclarecimentos sobre o eventual envolvimento no vazamento de dados, bem como para que informasse os motivos que causaram o problema, quais as providências para contê-lo, bem como o que fará para reparar os danos e evitar que a falha volte a acontecer;
- A ANPD afirmou que está apurando tecnicamente informações sobre o caso e que cooperará com os órgãos de investigação competentes para entender a origem do vazamento, a forma em que ele ocorreu, as medidas de contenção e de mitigação adotadas em um plano de contingência, bem como as possíveis consequências;
- O MPF-SP apontou que já recebeu ao menos uma representação individual para que o caso seja investigado;
- O MPDFT informou que está analisando o caso e que, por ora, não iria se pronunciar.

Em resposta à notificação do PROCON-SP, a Serasa Experian informou que a empresa observa o disposto na Lei Geral de Proteção de Dados para toda e qualquer operação com dados pessoais, bem como que mantém abrangente programa de segurança da informação e treinamento de seus funcionários.

Informou, ainda, que está sendo conduzida uma investigação aprofundada, mas que, até o momento, não há qualquer evidência de invasão em seus sistemas ou, ainda, que dados de crédito positivos ou negativos tenham sido expostos ilegalmente.

Para o diretor executivo do PROCON-SP, Fernando Capez, as informações apresentadas pela Serasa Experian teriam sido genéricas e insuficientes, sem especificação das medidas técnicas e organizacionais adotadas pela empresa, de forma que não descartaria a ocorrência de vazamento interno na empresa e ausência de base legal para o tratamento e uso de dados de forma indiscriminada.

A diretoria do órgão deixou claro que não descarta a possibilidade de aplicação de multa prevista no Código de Defesa do Consumidor – que pode chegar até o montante de R$ 10 milhões – após o encerramento da análise das informações prestadas pela Serasa Experian.

Pauta de atuação da SENACON em 2021 na proteção de dados pessoais e o estreitamento das relações com a ANPD

A SENACON e a ANPD têm promovido uma aproximação institucional para implementar atuação alinhada em relação ao tema de proteção de dados pessoais.

Nesse sentido, a SENACON formalizou um Núcleo dentro do Conselho Nacional de Defesa do Consumidor (CNDC), em busca de uma relação direta com a ANPD, para promoverem atividades conjuntas relacionadas à proteção de dados pessoais no âmbito de relações de consumo – garantindo, assim, não somente a proteção dos consumidores, mas também a segurança dos dados pessoais. Neste tema, o CNDC contará com o auxílio dos advogados Laura Schertel Mendes e Luciano Timm, especialistas em defesa do consumidor.

Além disso, há expectativa de que até março seja firmado um Acordo de Cooperação Técnica (ACT) para a proteção de dados dos consumidores, no qual a SENACON pretende compartilhar informações coletadas sobre as reclamações de consumidores relacionadas à proteção de dados pessoais, enquanto a ANPD fixará interpretações necessárias à aplicação da LGPD nos casos concretos. O intuito é buscar uniformizar os entendimentos e implementar uma atuação coordenada no endereçamento de reclamações de consumidores.

Em reunião realizada com a secretária nacional do Consumidor, Juliana Oliveira Domingues, o presidente da ANPD, Waldemar Gonçalves, revelou que a parceria entre as autoridades é muito positiva, pois auxiliará na organização da atuação específica de cada um desses atores do cenário de proteção de dados no Brasil.

Ainda, em entrevistas recentes concedidas, a secretária nacional do Consumidor informou que a SENACON já tem 42 processos de investigações administrativas envolvendo proteção de dados, além de constatar um aumento de casos que envolvem grandes vazamentos de dados dos consumidores. Destacou, ainda, que a Secretaria já trabalha para apurar provas e autorias desses vazamentos, não descartando a aplicação de sanções previstas no Código de Defesa do Consumidor (CDC).

A Secretaria também apontou estar atenta à atuação das *big techs*, em especial em razão de seu poder econômico, a fim de evitar a exposição ilícita de dados pessoais dos consumidores por meio de compartilhamento de dados e utilização de marketing direcionado, ressaltando que o tema demanda análise técnica e aplicação correta dos dispositivos do CDC aos novos cenários tecnológicos ora vivenciados.

PROCON-SP pede abertura de inquérito policial e STF determina a suspensão do site “fuivazado.com.br” no âmbito do inquérito das Fake News

O PROCON-SP encaminhou pedido de abertura de inquérito policial ao delegado-geral de Polícia do Estado de São Paulo para investigação das atividades do site “fuivazado.com.br”, o qual promete a confirmação – através de consulta através do número do CPF ou CNPJ e data de nascimento – sobre se os usuários foram afetados pelo “megavazamento” de dados pessoais de 220 milhões de brasileiros ocorrido no início do ano.

Segundo o PROCON-SP, o site teve acesso a mais de 223 milhões de CPFs e mais de 40 milhões de CNPJs constantes em listas ilegalmente disponibilizadas na internet, bem como pede doações em dinheiro aos seus usuários para a manutenção de suas atividades.

Contudo, para a Autoridade, o site (i) não esclareceria a necessidade ou finalidade da utilização dos dados pessoais dos usuários para a realização da consulta, bem como (ii) não demonstraria de que forma obteve acesso às listas com dados pessoais vazados.

A investigação pela Autoridade servirá para averiguar a possível violação à legislação relativa à proteção dos dados pessoais, bem como a eventual exploração comercial indevida por parte do site.

Paralelamente, o site foi retirado do ar após determinação do ministro do Supremo Tribunal Federal (STF) Alexandre de Moraes, no âmbito do Inquérito nº 4.781, chamado Inquérito das Fake News.

Segundo o ministro, mais do que informar aos usuários sobre os dados que foram vazados, o site estaria comercializando ilegalmente dados pessoais de autoridades nacionais e dos ministros do STF. Em razão disso, requereu a oitiva da pessoa identificada como responsável pelo site e a determinação para que empresas buscadoras de conteúdo retirassem imediatamente de seus resultados a remissão ao endereço de referido site. Desde então, o site segue fora do ar.

Decisões Internacionais

As diretrizes do Comitê Europeu sobre a notificação de violação de dados pessoais

O Comitê Europeu para a Proteção de Dados (EDPB) emitiu as “Diretrizes 01/2021”, no dia 14 de janeiro de 2021, sobre a notificação de violação de dados pessoais. Essas diretrizes foram emitidas com o intuito de complementar a orientação geral dada pelo Grupo de Trabalho do Artigo 29, através de orientação que utilize as experiências adquiridas desde a entrada em vigor do Regulamento Geral sobre a Proteção de Dados da União Europeia (GDPR). Seu objetivo é ajudar os controladores a lidar com violações de dados, informando os fatores que devem ser considerados durante a avaliação do risco.

O EDPB salienta que, como parte de qualquer tentativa de resolver uma violação, o controlador deve primeiro ser capaz de reconhecer uma. A esse respeito, comenta que as violações podem ser categorizadas de acordo com três frentes: (i) “Violação da confidencialidade” – na qual há um acesso não autorizado ou divulgação acidental de dados pessoais, (ii) “Violação da integridade” – pela qual há uma alteração não autorizada ou acidental de dados, e (iii) “Violação da disponibilidade” – na qual existe uma perda ou destruição de dados pessoais.

Uma violação pode, potencialmente, ter uma série de efeitos adversos sobre os indivíduos, que podem resultar em danos físicos, materiais ou psíquicos. O GDPR dispõe que isso pode incluir perda de controle sobre seus dados pessoais, limitação de seus direitos, discriminação, fraude, perda financeira, reversão não autorizada da pseudonimização, danos à reputação e perda de confidencialidade sobre dados protegidos por sigilo profissional. Por isso, ressalta o EDPB que uma das obrigações mais importantes do controlador é avaliar esses riscos para os direitos e as liberdades dos titulares, além de implementar medidas técnicas e organizacionais adequadas para resolvê-los.

A esse respeito, a regulação europeia exige que o agente de tratamento documente quaisquer violações de dados pessoais, seus efeitos e as medidas corretivas tomadas. Além disso, exige-se a notificação da violação de dados pessoais à autoridade nacional e a comunicação da violação ao titular, quando houver suscetibilidade de resultar em alto risco para os direitos e liberdades fundamentais.

As violações de dados são sintomas de um regime de segurança vulnerável e desatualizado, portanto, indicando deficiências a serem tratadas, segundo as Diretrizes. Antes que um controlador possa avaliar totalmente o risco decorrente de uma violação, a causa do problema deve ser identificada. Desse modo, há que se verificar também se as vulnerabilidades que deram origem ao incidente ainda estão presentes. Em muitos casos, o agente de tratamento consegue identificar que o incidente pode resultar em um risco e o notifica. Já em outros, não. Assim, recomenda-se que a notificação não seja adiada até que o impacto tenha sido totalmente avaliado, já que a avaliação pode acontecer ainda em paralelo à notificação.

Desse modo, a violação deve ser notificada quando o agente considerar que é provável que resulte em risco para os direitos e as liberdades do titular, devendo fazer essa avaliação no momento em que toma conhecimento da violação. As diretrizes são claras em orientar que não se deve esperar por um exame detalhado ou pelos primeiros passos da mitigação dos riscos para que se proceda à notificação.

Cada agente de tratamento deve ter planos para lidar com eventuais violações de dados pessoais, como recomenda o EDPB. A sua preparação quanto a questões de proteção de dados, com foco na gestão de violações, é essencial. Orienta-se a realização de treinamentos que devem ser repetidos regularmente, discutindo os últimos alertas sobre incidentes de segurança.

O Comitê orienta também sobre a elaboração antecipada, por cada organização, de um “manual” que funcionaria como uma fonte rápida de informações para permitir que os agentes mitigassem os riscos, sem demora. Isso garantiria que, se uma violação de dados pessoais ocorresse, os integrantes da organização saberiam o que fazer e o incidente, provavelmente, seria tratado de maneira mais veloz. Por fim, as Diretrizes definem a documentação sobre a violação de dados, como uma obrigação independente dos riscos inerentes à violação, devendo ser realizada em todos os casos.

Reconhecimento Facial: rostos como códigos de barra

A Autoridade de Proteção de Dados Holandesa emitiu um aviso formal a um supermercado em razão do uso da tecnologia de reconhecimento facial. A tecnologia havia sido desativada anteriormente, todavia, o supermercado tinha intenção de voltar a usá-la.

Alguns pontos do supermercado são a proteção aos clientes e funcionários, bem como a prevenção ao furto. A tecnologia, vinculada às câmeras de entrada do supermercado, escaneava os rostos das pessoas que entravam e os comparava com o banco de dados de pessoas que haviam sido banidas do supermercado.

A vice-presidente da Autoridade Holandesa, ao se pronunciar sobre o caso, disse que seria inaceitável o uso de tecnologia de reconhecimento facial pelo supermercado, bem como por qualquer outra loja na Holanda. Complementou que o reconhecimento facial faz das pessoas "códigos de barra ambulantes", além de ser realizado sem o consentimento. Segundo a vice-presidente, a tecnologia de reconhecimento facial expõe os rostos em um mecanismo de pesquisa, o qual poderá ser relacionado com o nome da pessoa ou qualquer outro dado pessoal, inclusive aqueles disponíveis em redes sociais.

Na Holanda, como a tecnologia usa dados biométricos, ela só é permitida em duas hipóteses: (i) quando há explícito consentimento do titular dos dados para que estes sejam tratados pela tecnologia de reconhecimento facial; (ii) quando a tecnologia for necessária para autenticação ou para fins de segurança na medida em que haja interesse público envolvido, como na segurança de uma central nuclear – exemplo dado pela Autoridade de Proteção de Dados Holandesa.

Na realidade brasileira, cabe lembrar que reconhecimento facial já foi alvo de discussões. No começo de 2019, um homem, procurado pela polícia, foi preso após ter seu rosto reconhecido por câmera de reconhecimento facial no carnaval de Salvador. No mesmo ano, no Rio de Janeiro, uma mulher foi detida por engano em razão de falha no sistema de reconhecimento facial da Polícia Militar. Até mesmo, no começo do ano passado, o Tribunal de Justiça de São Paulo determinou que o Metrô de São Paulo desse explicações sobre o projeto de reconhecimento facial por câmeras e o tratamento de dados a ser realizado por essa tecnologia.

Fonte: https://edpb.europa.eu/news/national-news/2021/dutch-dpa-issues-formal-warning-supermarket-its-use-facial-recognition_en

Empresa de reconhecimento facial americana realiza ilicitamente vigilância em massa no Canadá

A empresa Clearview AI permitia, por meio de seus serviços, que organizações policiais e comerciais combinassem fotos de pessoas desconhecidas com seu banco de dados de mais de 3 bilhões de imagens, incluindo de canadenses e crianças para fins investigativos.

Em investigação realizada pela Autoridade de Proteção de Dados Canadense, foi apurado que essa permissão possibilitava a criação potencial de danos significativos aos indivíduos, os quais não tinham qualquer envolvimento com crimes e cujas fotos eram coletadas, divulgadas e disponibilizadas pela Clearview AI. A Autoridade Canadense entendeu que houve coleta de dados biométricos altamente sensíveis sem qualquer conhecimento e consentimento de seus titulares.

Embora a Clearview AI alegue que as leis de privacidade canadenses não se aplicam a suas atividades, por não haver relação direta entre a empresa e o Canadá, e que o consentimento não era necessário, uma vez que as informações coletadas estavam disponíveis publicamente, a Autoridade Canadense rejeitou esses e demais argumentos da empresa, a qual parou de fornecer seus serviços no mercado canadense no início da investigação.

No cenário brasileiro, ainda que o tratamento de dados não ocorra no território brasileiro ou que os agentes de tratamento – controladores e operadores – não estejam localizados no Brasil, a Lei Geral de Proteção de Dados (LGPD) é aplicável, tendo em vista seu escopo extraterritorial. Desse modo, caso os dados pessoais, inclusive imagens, tenham sido coletados no Brasil ou caso o tratamento tenha por objetivo o tratamento de dados de indivíduos localizados no território nacional – tal como a vigilância de indivíduos que estejam no Brasil – a LGPD será aplicável.

Fonte: https://www.priv.gc.ca/en/opc-news/news-and-announcements/2021/nr-c_210203/

Extra

Avanços Normativos diversos

A Futura Lei de Proteção de Informação Pessoal da China

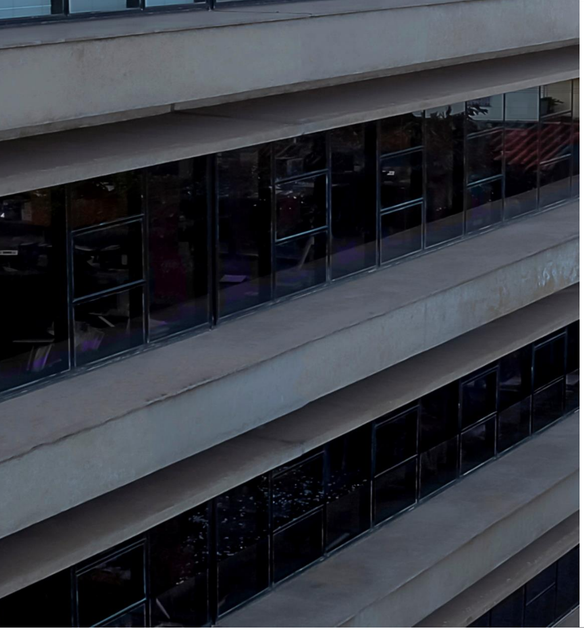
O projeto de lei de proteção de informação pessoal da China (Personal Information Protection Law ou PIPL), publicado em outubro de 2020, conta com 8 capítulos e 70 artigos sobre tratamento de informação pessoal, direitos dos titulares, deveres e responsabilidade envolvendo o tratamento de informações pessoais, entre outros assuntos. Ainda que não tenha sido publicado, a PIPL já chama atenção das empresas para a conformidade com suas disposições.
Com clara influência do Regulamento Geral sobre a Proteção de Dados (GDPR) e semelhança com a Lei Geral de Proteção de Dados (LGPD), "informação pessoal" abrange qualquer informação registrada, por meio eletrônico ou outros meios, relacionada à pessoa natural identificada ou identificável.

Mais abrangente do que as disposições da GDPR e da LGPD, segundo a PIPL, informação pessoal sensível seria aquela que, se divulgada ou usada ilicitamente, possa causar discriminação contra pessoas naturais ou grave dano à segurança pessoal ou segurança patrimonial, incluindo informação sobre raça, etnia, crenças religiosas, características biométricas individuais, saúde, contas bancárias e localização. Também, ao contrário da maioria das leis de proteção de dados, a PIPL não diferencia as posições de controladores e operadores, se referindo a todos que realizam o tratamento de informação como operadores.

Quanto ao escopo territorial da PIPL, a lei, se aprovada, será aplicável a atividades de tratamento realizadas no território chinês ou a atividades que, mesmo realizadas fora da China, tratam informações cujo objetivo é o fornecimento de produtos e serviços para pessoa natural localizada no território chinês ou a análise e avaliação de atividades de pessoas naturais localizadas no território chinês. Além dessas hipóteses, a PIPL será aplicável também em circunstâncias previstas em leis ou normas administrativas.

Embora ainda necessite de aprovação, a PIPL já pode implicar em algumas mudanças organizacionais, a fim de atender a conformidade com a futura lei, nas relações entre empresas brasileiras e pessoas naturais localizadas na China, ou entre empresas brasileiras e outras empresas que realizam tratamentos de informações sujeitas à PIPL.

Fontes: https://iapp.org/news/a/china-personal-information-protection-bill-a-pragmatic-but-yet-to-be-improved-approach/ | https://www.china-briefing.com/news/data-privacy-china-personal-information-protection-law-it-compliance-considerations/ | https://assets.kpmg/content/dam/kpmg/cn/pdf/en/2020/11/overview-of-draft-personal-information-protection-law-in-china.pdf



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/