A Year in Privacy

TRILHA DO PROCESSO ADMINISTRATIVO

ANÁLISE DE CASOS

Guia 06

Autores:
Ana Julia Gusukuma
Dandara Ramos Silvestre
Adele Mendes Weinberg

Revisores:
Adriane Loureiro Novaes
Fernando Bousso

b/luz

sumário clicável

SUMÁRIO

← Voltar ao sumário

1. INTRODUÇÃO

Para facilitar a compreensão das fases do processo administrativo, este guia apresenta uma análise aprofundada de casos reais de sanções impostas pela Autoridade Nacional de Proteção de Dados (ANPD).

Por meio da análise dos relatórios de instrução que embasaram as sanções aplicadas a diversas organizações, como Telekall Inforservices, Instituto de Pesquisa Jardim Botânico do Rio de Janeiro (JBRJ), Secretaria de Educação do Distrito Federal (SEEDF), Secretaria de Estado de Saúde de Santa Catarina (SES-SC), Secretaria de Desenvolvimento Social, Criança e Juventude de Pernambuco (SDSCJ-PE) e Instituto de Assistência Médica ao Servidor Público Estadual de São Paulo (IAMSPE), destacamos as similaridades e diferenças entre os casos.

Esta abordagem proporciona uma visão clara do raciocínio e dos critérios adotados pela ANPD na aplicação das sanções, oferecendo uma perspectiva prática das implicações do não cumprimento das regras da Lei Geral de Proteção de Dados Pessoais (LGPD).

← Voltar ao sumário

2. ANÁLISE DE CASOS

2.1. PROCESSO Nº 00261.000489/2022-62 - Telekall Infoservices

A Telekall Inforservices, microempresa do setor privado de telecomunicações, foi acusada de ter oferecido a candidatos às eleições municipais uma lista de contatos de WhatsApp de eleitores de Ubatuba/SP para o envio de materiais de campanha eleitoral, sem uma base legal para o tratamento de dados. A empresa também não apresentou comprovação do registro das operações de tratamento de dados pessoais, não submeteu o relatório de impacto à proteção de dados pessoais referente a essa operação e não comprovou a nomeação de um encarregado de proteção de dados.

Em 28 de fevereiro de 2021, a Telekall Infoservices foi notificada pela ANPD sobre uma investigação relacionada à comercialização de bases de dados. Em sua defesa, a empresa alegou que não havia sido contratada para prestar o serviço, mas essa justificativa foi considerada insuficiente. A ANPD tentou contatar a empresa novamente, solicitando a apresentação de determinados documentos. No entanto, mesmo após o segundo aviso, a empresa não forneceu as informações requisitadas.

No auto de infração, a ANPD apontou as seguintes violações:

(I) HIPÓTESE LEGAL DE TRATAMENTO DE DADOS PESSOAIS (ART. 7º DA LGPD)

Embora a Telekall Infoservices não tenha apresentado uma base legal para o tratamento de dados pessoais, conforme exigido pelo art. 7º da LGPD, não há evidências de que essa infração tenha impedido o exercício dos direitos dos titulares ou causado danos materiais ou morais, como fraudes ou uso indevido de identidade.

Gravidade da infração: Leve

A ANPD classificou a infração como leve, conforme o Regulamento de Dosimetria e Aplicação de Sanções Administrativas ("Regulamento de Dosimetria").

Sanção aplicada: multa simples

Embora a infração ao art. 7º da LGPD tenha sido considerada leve pelo Regulamento de Dosimetria, a ANPD entende que a aplicação de uma advertência é desproporcional, uma vez que o artigo infringido é fundamental para a legitimidade do tratamento de dados. À luz disso, a aplicação de multa simples é tida como mais adequada, especialmente devido à intenção do infrator de obter vantagem econômica com o ato infrator.[1] Além disso, a tentativa da empresa de obter vantagem econômica com suas atividades agravou a infração, justificando a aplicação de uma multa de R$ 7.200,00 (sete mil e duzentos reais) à Telekall Infoservices.

(II) INDICAÇÃO DO ENCARREGADO (ART. 41 DA LGPD)

No caso em questão, apesar das múltiplas solicitações da ANPD para a confirmação da nomeação do encarregado, a Telekall Inforservices não atendeu a essa exigência. Diante da ausência desse documento, a ANPD concluiu que a empresa não nomeou um encarregado, em violação ao art. 41 da LGPD.

Gravidade da infração: Leve

De acordo com a ANPD não há provas que levem à conclusão de que a falta de comprovação da indicação do encarregado impediu ou limitou o exercício de direitos ou a utilização do serviço; ocasionou danos materiais ou morais aos titulares; causou fraudes financeiras; ou gerou o uso indevido de identidade[2]. Dessa forma, a ANPD entende que as consequências dessa infração não tiveram um impacto muito abrangente.

Sanção aplicada: Advertência

Conforme o art. 9º, I, do Regulamento de Dosimetria, a advertência é a sanção aplicável em casos de infrações leves ou médias.

1 Resolução CD/ANPD nº 4, de 24 de fevereiro de 2023. Aprova o Regulamento de Dosimetria e Aplicação de Sanções Administrativas. Art. 10, II. Diário Oficial da União: Brasília/ DF. Disponível em: https://www.gov.br/anpd. Acesso em: 11 set. 2024

2 Regulamento de Dosimetria e Aplicação de Sanções Administrativas. Art. 8º, § 2º.

(III) NÃO FORNECIMENTO DE INFORMAÇÕES SOLICITADAS PELA ANPD (ART. 5º, INCISO I, DO REGULAMENTO DE FISCALIZAÇÃO)

Ficou constatado que, mesmo após as solicitações da ANPD, a Telekall Inforservices continuou a oferecer em seu site contatos de WhatsApp, indicando que a empresa seguia ofertando tais serviços no mercado. Além disso, a ANPD, por meio de ofícios e despachos, solicitou diversos documentos. No entanto, a resposta fornecida pela Telekall foi considerada insuficiente, e a ANPD requisitou informações adicionais. Embora a empresa tenha acusado o recebimento do pedido, nenhuma resposta foi encaminhada.

Gravidade da infração: Grave

A ANPD considerou que a ausência de fornecimento dos documentos, dados e informações solicitados para a avaliação do tratamento de dados pessoais resultou na obstrução do processo de fiscalização. Conforme o art. 8º, §3º, inciso II, do Regulamento de Dosimetria, essa conduta configura uma infração grave.

O descumprimento da obrigação de colaborar com a autoridade reguladora resultou na violação do art. 5º, inciso I, do Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador ("Regulamento de Fiscalização")[3], que estabelece a cooperação obrigatória do agente regulado.

Sanção aplicada: multa simples

De acordo com o art. 10, inciso II, do Regulamento de Dosimetria, infrações graves resultam na aplicação de multa. Inicialmente, o valor da multa foi calculado em R$ 2.880,00. No entanto, o regulamento estabelece um valor mínimo de R$ 12.000,00 para infrações graves. Considerando que a Telekall é uma microempresa e respeitando o limite legal de 2% do faturamento, o valor final da multa foi ajustado para R$ 7.200,00.[4]

A decisão completa pode ser acessada neste link.

3 Regulamento de Fiscalização e Aplicação de Sanções: art. 55. BRASIL. Resolução CD/ANPD nº 1/2021. Diário Oficial da União: Brasília/DF. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/regulamentacoes-da-anpd/resolucao-cd-anpd-no1-2021. Acesso em 18 de agosto de 2024.

4 Regulamento de Dosimetria e Aplicação de Sanções Administrativas. Art. 10, II.

← Voltar ao sumário

2.2. PROCESSO Nº 00261.000574/2022-21 - Instituto de Pesquisa Jardim Botânico do Rio de Janeiro

O Instituto de Pesquisa Jardim Botânico do Rio de Janeiro (JBRJ) é uma instituição pública vinculada ao governo do estado do Rio de Janeiro, dedicada ao estudo, pesquisa e conservação da natureza, com foco especial em botânica.

O processo foi instaurado pela Coordenação-Geral de Fiscalização (CGF/ANPD) para investigar possíveis violações à LGPD, após a divulgação de notícias sobre um suposto vazamento de dados envolvendo órgãos públicos, incluindo o JBRJ.

A CGF solicitou esclarecimentos ao Instituto, concedendo um prazo de 30 dias para que informasse a ANPD e os afetados sobre o incidente ou justificasse a falta de notificação. O Instituto não apresentou a notificação nem justificou sua omissão. Em sua defesa, o JBRJ alegou que não recebeu a notificação devido a um erro de envio e que o ataque não comprometeu dados pessoais, afirmando ainda que seguiu orientações das autoridades competentes. O Instituto destacou a criação de um Comitê de Privacidade e a implementação de um projeto de adequação à LGPD. O processo foi suspenso e retomado em abril de 2023, quando o Instituto reforçou suas medidas de conformidade.

No auto de infração, a ANPD apontou as seguintes violações:

(I) COMUNICAÇÃO DO INCIDENTE DE SEGURANÇA À ANPD E AOS TITULARES (ART. 48 DA LGPD)

No caso concreto, a ANPD não aplicou sanção, entendendo que o incidente de segurança envolveu apenas dados de pesquisa, sem abranger dados pessoais. Assim, a defesa do JBRJ foi acolhida, pois, sem o envolvimento de dados pessoais, não há obrigação de notificar a autoridade e os titulares. Portanto, não houve violação ao art. 48 da LGPD.

Gravidade da infração: Não aplicável

Sanção aplicada: Não aplicável

← Voltar ao sumário

(II) NÃO FORNECIMENTO DE INFORMAÇÕES SOLICITADAS PELA ANPD (ART. 5º, INCISO I, DO REGULAMENTO DE FISCALIZAÇÃO)

Embora a ANPD tenha alegado que o JBRJ não atendeu às suas requisições durante o processo de fiscalização, o JBRJ, em sua defesa, afirmou que não recebeu a notificação exigindo a apresentação de documentos relacionados ao incidente de segurança.

Após verificação, a ANPD constatou que não havia evidências de que o JBRJ recebeu o ofício, pois o aviso de recebimento não foi encontrado nos autos do processo ou junto aos Correios. Sem essa prova, não há confirmação de que o Instituto foi formalmente notificado.

Diante da ausência de comprovação de recebimento, a ANPD concluiu que não há materialidade suficiente para caracterizar a infração, já que o JBRJ não foi devidamente informado da requisição. Portanto, a infração ao art. 5º não foi configurada, conforme inicialmente apontado no Auto de Infração.

Considerando a não configuração da infração ao art. 48 da LGPD e a ausência de violação ao art. 5º do Regulamento de Fiscalização, a ANPD recomendou o arquivamento do Processo Administrativo Sancionador.

Gravidade da infração: Não aplicável

Sanção aplicada: Não aplicável

A decisão completa pode ser acessada neste link.

← Voltar ao sumário

2.3. PROCESSO Nº00261.001192/2022-14 – Secretaria de Educação do Distrito Federal

A Secretaria de Educação do Distrito Federal (SEEDF)
é o órgão público responsável por coordenar as atividades relacionadas à educação pública no Distrito Federal, desempenhando um papel essencial na organização do sistema educacional, desde a educação infantil até o ensino fundamental e médio.

A Coordenação-Geral de Fiscalização (CGF)
identificou que a SEEDF expôs indevidamente dados pessoais de estudantes devido a uma falha de segurança no formulário de inscrição do Programa Educação Precoce. Documentos comprovaram que dados cadastrais e de saúde de mais de 3.000 candidatos e seus responsáveis ficaram acessíveis ao público.

Em novembro de 2021, a CGF solicitou que a SEEDF corrigisse a falha e fornecesse informações adicionais, como um relatório de impacto sobre a proteção de dados e dados do encarregado. Embora a SEEDF tenha tomado algumas medidas, a CGF considerou-as insuficientes e determinou a notificação tanto da ANPD quanto dos titulares dos dados, conforme disposições do artigo 48 da LGPD.

A SEEDF notificou a ANPD em janeiro de 2022, mas não informou os titulares, alegando falta de provas suficientes e o risco de gerar alarme desnecessário. A CGF reiterou a necessidade de notificação aos titulares e estabeleceu um prazo para o cumprimento. A SEEDF, no entanto, não respondeu adequadamente, o que resultou em um novo aviso da ANPD em maio de 2022, aumentando o risco de sanções por não conformidade com a LGPD.

O Auto de Infração aponta o descumprimento dos seguintes dispositivos legais:

(I) COMUNICAÇÃO DO INCIDENTE AOS TITULARES AFETADOS (ART. 48 DA LGPD)

A SEEDF foi acusada de não comunicar de forma adequada e dentro do prazo aos titulares sobre a ocorrência de um incidente de segurança, conforme exigido pelo art. 48 da LGPD. A Secretaria também alegou que a comunicação não seria necessária, pois os dados não foram divulgados em canais sob sua responsabilidade e não houve prejuízo aos titulares ou à administração pública.

A ANPD refutou essas alegações, destacando que a SEEDF levou oito meses para comunicar o incidente aos titulares, mesmo com prazos claros estabelecidos pela ANPD. A justificativa de dificuldades técnicas foi considerada inaceitável, já que a SEEDF possuía os e-mails dos titulares afetados e poderia ter realizado o envio manualmente.

Gravidade da infração: Grave

comunicação individualizada aos titulares foi considerada um impacto significativo sobre os direitos e interesses dos afetados, justificando a classificação inicial da infração como média. No entanto, a gravidade foi aumentada devido ao envolvimento de dados pessoais sensíveis, incluindo informações de saúde, e dados de crianças e adolescentes.

Sanção aplicada: Advertência

Apesar da gravidade da infração, a aplicação de multa foi descartada, uma vez que o art. 52, §3º da LGPD exclui a possibilidade de aplicar multas a órgãos público. No mais, a aplicação da advertência a infrações leves ou médias, ou em casos que exijam medidas corretivas também é restrita[5]. Entretanto, sem outra sanção adequada, a advertência foi considerada o único meio de evitar que a infração ficasse sem qualquer punição, respeitando o princípio da proporcionalidade.

(II) NÃO UTILIZAÇÃO DE SISTEMA ADEQUADO AO TRATAMENTO DE DADOS PESSOAIS (ART. 49 DA LGPD)

Após ser acusada de não atender aos requisitos de segurança da LGPD, a SEEDF justificou o uso do Google Forms durante a pandemia de Covid-19 devido à necessidade urgente de adaptação. A rápida implementação da plataforma, sem o devido treinamento da equipe técnica, resultou em erros de configuração e na exposição indevida de dados pessoais. A investigação revelou que a falha não estava no sistema em si, mas na administração, pois a SEEDF não adotou as medidas necessárias para garantir a segurança de dados, conforme o artigo 46 da LGPD.

Apesar da ausência de medidas adequadas, foi reconhecido que a situação excepcional da pandemia constituiu força maior, rompendo o nexo causal para responsabilizar a SEEDF pelo descumprimento do artigo 46. Embora a falta de treinamento tenha contribuído para o incidente, o princípio da razoabilidade e as circunstâncias excepcionais levaram à reconsideração da autuação, ajustando a aplicação das sanções administrativas ao contexto da crise.

(III) AUSÊNCIA DE COMPROVAÇÃO DE REGISTRO DAS OPERAÇÕES DE TRATAMENTO DE DADOS PESSOAIS (ART. 37 DA LGPD)

A SEEDF foi autuada por não manter o Registro de Operações de Tratamento de Dados, conforme exige o artigo 37 da LGPD. Em sua defesa administrativa, apresentou um documento intitulado “Registro de Operação de Tratamento dos Dados Afetados pelo Incidente”, detalhando a análise do incidente de segurança e as medidas corretivas adotadas, como a suspensão de acessos e a exclusão dos dados expostos.

5 Regulamento de Dosimetria e Aplicação de Sanções Administrativas. Art. 9º.

No entanto, a ANPD apontou que, apesar de ter solicitado esse relatório antes do início do processo sancionador, a SEEDF não o apresentou prontamente. Quando finalmente enviado, o relatório foi considerado insuficiente, pois limitava-se a descrever as ações tomadas após o incidente, sem incluir o registro contínuo das operações de tratamento de dados pessoais, conforme exige o artigo 37. A ANPD destacou que o registro de operações de tratamento deve ser mantido de forma contínua e não apenas em resposta a incidentes de segurança.

Gravidade da infração: Leve

Considerando a ausência de evidências de que a falta desse Relatório tenha limitado os direitos dos titulares de dados ou causado danos materiais ou morais, e não havendo circunstâncias agravantes ou atenuantes identificadas, a ANPD classificou a infração como leve.[6]

Sanção aplicada: Advertência

De acordo com o art. 9º, inciso I, do Regulamento de Dosimetria, a advertência pode ser aplicada como sanção em casos de infração leve ou média.

(IV) NÃO FORNECIMENTO DO RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS (ART. 38 DA LGPD)

A SEEDF também foi autuada por não ter elaborado e apresentado o Relatório de Impacto à Proteção de Dados (RIPD), conforme solicitado. De acordo com o art. 38 da LGPD, a elaboração do RIPD é essencial para documentar os processos de tratamento de dados pessoais que possam gerar riscos às liberdades civis e aos direitos fundamentais dos titulares.

Por meio da Nota Técnica nº 40/2022, a ANPD exigiu a apresentação do RIPD. No entanto, a SEEDF não o apresentou, mesmo após meses da solicitação inicial, configurando infração ao art. 38 da LGPD.

Gravidade da infração: Leve

A infração foi classificada como leve, pois não houve evidências de que a ausência do RIPD tenha causado prejuízos significativos aos direitos dos titulares de dados ou agravado sua situação[7]. Além disso, não foram identificados indícios de que essa falha tenha impactado substancialmente os interesses fundamentais dos titulares.

6 Regulamento de Dosimetria e Aplicação de Sanções Administrativas. Art. 8º, §1º e o art. 9º, I.

7 Regulamento de Dosimetria e Aplicação de Sanções Administrativas. Art. 8º, § 1º

← Voltar ao sumário

Sanção aplicada: Advertência

Com base no art. 9º, inciso I, do Regulamento de Dosimetria, a sanção adequada ao caso foi a aplicação de uma advertência.

(V) NÃO FORNECIMENTO DE INFORMAÇÕES SOLICITADAS PELA ANPD (ART. 5º, INCISO I, DO REGULAMENTO DE FISCALIZAÇÃO)

A ANPD, por meio da Nota Técnica nº 40/2022, exigiu a apresentação de um plano de gestão de incidentes de segurança da informação. No entanto, a SEEDF não apresentou o documento, tampouco informou se o possuía. A ausência desse plano dificultou a avaliação, por parte da ANPD, das medidas adotadas para prevenir e mitigar os efeitos de incidentes de segurança, configurando, assim, uma infração ao art. 5º, inciso I, do Regulamento de Fiscalização.

Gravidade da infração: grave

A ANPD entendeu que o descumprimento do dever de fornecer documentos configurou obstrução à fiscalização, classificando a infração como grave.

Sanção aplicada: Advertência

O Regulamento de Dosimetria prevê a aplicação de multas para infrações graves, porém, conforme o art. 52, §3º, da LGPD, a aplicação de multas é vedada a órgãos públicos. Dessa forma, como as sanções mais severas não são aplicáveis, a única sanção possível foi a advertência. A penalidade final foi definida com base no princípio da proporcionalidade.

A decisão completa pode ser acessada neste link.

2.4. PROCESSO Nº 00261.001886/2022-51 – SECRETARIA DE ESTADO DE SAÚDE DE SANTA CATARINA

Trata-se de um incidente de segurança, ocorrido em agosto de 2021, comunicado pela Secretaria de Estado de Saúde de Santa Catarina (SES-SC), que envolveu a exfiltração de 4GB de dados sensíveis de pacientes e prestadores de serviço do SUS.

As informações vazadas incluíam nome, CPF, endereço, telefone e dados médicos, impactando aproximadamente 48 mil titulares. O incidente foi causado por uma falha de segurança durante uma manutenção emergencial em um servidor, que resultou na publicação indevida dos dados na internet.

Entre 2021 e 2022, a ANPD emitiu diversos despachos, solicitando o cumprimento de determinações e maior clareza na comunicação pública do incidente. Contudo, mesmo após orientações e a adoção de medidas preventivas, a SES-SC não atendeu plenamente às determinações da ANPD, levando à abertura de um Processo Administrativo Sancionador.

(I) COMUNICAÇÃO DO INCIDENTE AOS TITULARES AFETADOS (ART. 48 DA LGPD)

Embora a SES-SC tenha comunicado o incidente por meio de um aviso em seu site, a entidade justificou a ausência de uma comunicação individual aos titulares afetados pela falta de dados de contato atualizados. No entanto, a ANPD considerou essa justificativa insuficiente para cumprir as disposições do art. 48 da LGPD, que exige a notificação individual aos titulares sobre incidentes de segurança.

A ANPD ressaltou que a falha na comunicação individualizada, especialmente em casos de exposição de dados pessoais em ambientes não controlados, incluindo dados sensíveis, como os de saúde, pode acarretar prejuízos significativos aos titulares. Sem a devida notificação, os titulares são impedidos de adotar medidas preventivas contra possíveis danos, como uso indevido de identidade, fraudes financeiras e outros riscos decorrentes da exposição de seus dados.

Gravidade da infração: grave

A ANPD entendeu que a falta de comunicação individualizada aos titulares afetados pelo incidente impacta significativamente os direitos e interesses dos envolvidos, classificando a infração como de gravidade média.[8] A gravidade foi ainda majorada devido à presença de dados pessoais sensíveis.[9]

8 Regulamento de Dosimetria e Aplicação de Sanções Administrativas. Art. 8º, 2º.

9 Regulamento de Dosimetria e Aplicação de Sanções Administrativas. Art. 8º, §3º, "d"

Sanção aplicada: Advertência com medidas corretivas

Conforme o art. 9º, inciso II, do Regulamento de Dosimetria, a advertência é apropriada quando há necessidade de implementar medidas corretivas. Junto à sanção, foram impostas as seguintes medidas:

- Manter a comunicação sobre o incidente na página inicial do site por mais 90 dias; e
- Realizar uma comunicação individualizada aos titulares identificados no arquivo vazado, utilizando a ferramenta Notifica-BR.

(II) NÃO FORNECIMENTO DE INFORMAÇÕES SOLICITADAS PELA ANPD (ART. 5º, INCISO I, DO REGULAMENTO DE FISCALIZAÇÃO)

Após solicitação da ANPD, a SES-SC não forneceu o relatório de tratamento do incidente nem os registros de acesso (logs) necessários para a devida apuração do incidente de segurança, mesmo após a concessão de um prazo específico para isso. A SES-SC justificou que tais informações estavam sob a responsabilidade do operador de tratamento, o CIASC - Centro de Informática e Automação do Estado de Santa Catarina S.A. No entanto, a ANPD ressaltou que essa justificativa não isenta o controlador de suas obrigações, sendo o controlador responsável por fornecer as informações requisitadas, independentemente de estarem sob a posse do operador.

A ANPD entendeu que a ausência do relatório técnico impediu uma avaliação adequada das medidas técnicas adotadas para prevenir e mitigar os efeitos do incidente. Diante disso, a falta dessas informações foi considerada obstrução à atividade de fiscalização, conforme estabelecido no art. 6º do Regulamento de Fiscalização.

Gravidade da infração: grave

A ANPD considerou que o descumprimento do dever de fornecer os documentos solicitados configurou obstrução à fiscalização, classificando a infração como grave. [10]

Sanção aplicada: Advertência

Embora a multa simples seja a sanção usual para infrações graves [11], a ANPD optou por não aplicar essa penalidade no caso da SES-SC, em razão do caráter público da entidade[12]. Assim, a única sanção possível foi a advertência.

10 Regulamento de Dosimetria e Aplicação de Sanções Administrativas. Art. 8º, §3º, II,

11 Regulamento de Dosimetria e Aplicação de Sanções Administrativas. Art. 10, II

12 Regulamento de Dosimetria e Aplicação de Sanções Administrativas. Art. 3º, §5º,

(III) NÃO ELABORAÇÃO DE RELATÓRIO DE IMPACTO (ART. 38 DA LGPD)

A SES-SC foi notificada pela ANPD para elaborar um Relatório de Impacto à Proteção de Dados (RIPD), devido à sensibilidade dos dados tratados, conforme previsto no art. 38 da LGPD. O controlador solicitou um prazo de dois meses para a conclusão do relatório e, mesmo com o deferimento desse prazo, o RIPD não foi entregue.

Gravidade da infração: Leve

A ausência da apresentação do RIPD não resultou em impacto significativo sobre os direitos e interesses fundamentais dos titulares, motivo pelo qual a infração não foi considerada de gravidade média ou grave. Dessa forma, a infração foi classificada como leve, com caráter residual.

Sanção aplicada: Advertência

Embora a aplicação de multa simples seja possível em casos de descumprimento das medidas impostas,[13] a ANPD decidiu afastar essa penalidade no caso da SES-SC, considerando o caráter público da entidade[14]. Assim, a única sanção aplicável foi a advertência.

(IV) FALHA AO IMPLEMENTAR MECANISMOS DE SEGURANÇA ADEQUADOS (ART. 49 DA LGPD)

No caso, foi constatado que a SES-SC não implementou mecanismos básicos de segurança para proteger sua base de dados, violando o art. 49 da LGPD. Essa falha permitiu que terceiros não autorizados acessassem e publicassem dados pessoais na internet. A ANPD destacou que a ausência de controle de acesso e de registros de acesso ao banco de dados impediu a verificação completa da extensão da violação, mesmo após um ano da descoberta do incidente.

A Autoridade ressaltou que o incidente envolveu dados pessoais de saúde, que demandam proteção ainda mais rigorosa. A falta de medidas adequadas para proteger essas informações pode gerar danos significativos, como fraudes financeiras, uso indevido de identidade, além de perturbações, como ligações indevidas e dificuldades em processos de autenticação.

13 Regulamento de Dosimetria e Aplicação de Sanções Administrativas. Art. 10, I

14 Regulamento de Dosimetria e Aplicação de Sanções Administrativas. Art. 3º, §5º

Gravidade da infração: grave

A não implementação de medidas de segurança adequadas foi considerada como um fator que possibilitou a concretização do incidente, impactando significativamente os direitos e interesses dos titulares afetados. Dessa forma, a infração foi classificada como de gravidade média.[15] A gravidade foi ainda aumentada devido à presença de dados pessoais sensíveis.[16]

Sanção aplicada: Advertência com medidas corretivas

Conforme o art. 9º, inciso II, do Regulamento de Dosimetria, a sanção de advertência é apropriada quando há necessidade de medidas corretivas. Consta nos autos que a SES-SC já implementou medidas de segurança adicionais. A ANPD também ressaltou que, apesar da possibilidade de aplicação de multa simples para infrações graves [17], decidiu afastar essa penalidade no caso da SES-SC, considerando o caráter público da entidade.[18]

A decisão completa pode ser acessada neste link.

2.5. PROCESSO Nº00261.001963/2022-73 - SECRETARIA DE DESENVOLVIMENTO SOCIAL, CRIANÇA E JUVENTUDE DE PERNAMBUCO

Trata-se de um incidente de segurança envolvendo dados pessoais, reportado pela Secretaria de Desenvolvimento Social, Criança e Juventude de Pernambuco (SDSCJ-PE). O incidente, ocorrido em maio de 2022, resultou na exposição de dados de usuários do serviço de transporte intermunicipal para pessoas com deficiência. Uma planilha contendo os dados dos cadastrados no programa de gratuidade de transporte foi exposta no site da Secretaria, permitindo o acesso sem a necessidade de senha.

A confidencialidade de informações sensíveis de 413 pessoas com deficiência, incluindo crianças e adolescentes, foi comprometida. Os dados expostos incluíam informações de saúde, documentos de identificação oficial, endereço e e-mail. O incidente ocorreu devido a uma falha no controle de acesso em abril de 2022, afetando os inscritos no "Programa PE Livre Acesso Intermunicipal", que concede gratuidade no transporte intermunicipal a pessoas com deficiência física, sensorial e mental.

15 Regulamento de Dosimetria e Aplicação de Sanções Administrativas. Art. 8º, 2º.

16 Regulamento de Dosimetria e Aplicação de Sanções Administrativas. Art. 8º, §3º, "d"

17 Regulamento de Dosimetria e Aplicação de Sanções Administrativas. Art. 3º, §5º

18 Regulamento de Dosimetria e Aplicação de Sanções Administrativas. Art. 3º, §5º,

Dada a gravidade do incidente e a natureza dos dados expostos, a ANPD concluiu que havia um risco significativo de danos aos titulares, especialmente considerando a vulnerabilidade do grupo afetado. O incidente foi classificado como grave, e a ANPD determinou que a Secretaria notificasse individualmente os titulares e fornecesse um relatório detalhado do ocorrido.

No entanto, a SDSCJ-PE não atendeu às exigências da ANPD, incluindo a falha em comunicar os titulares.

(I) COMUNICAÇÃO DO INCIDENTE AOS TITULARES AFETADOS (ART. 48 DA LGPD)

A ANPD considerou que a comunicação indireta realizada pelo controlador, por meio de uma nota publicada no site, foi insuficiente para alcançar os titulares afetados pelo incidente. Segundo a ANPD, a nota foi postada em uma página sem conexão direta com a plataforma onde os titulares fornecem seus dados e utilizam os serviços públicos, tornando improvável que fosse acessada por eles.

A comunicação do incidente foi avaliada como inadequada pela ANPD, já que não seguiu o §1º do art. 48 da LGPD, que exige a notificação individualizada dos titulares. Dado que o número de titulares afetados era limitado e que o controlador possuía os endereços físicos e eletrônicos desses titulares, a ANPD concluiu que uma comunicação individualizada seria plenamente viável e razoável.

A ausência dessa comunicação prejudicou os direitos fundamentais dos titulares, especialmente devido à exposição de dados sensíveis, incluindo informações de saúde, e de dados de crianças e adolescentes, o que aumenta significativamente o risco de danos, como fraudes e discriminação. A ANPD também destacou que a exposição dos dados poderia comprometer o direito dos titulares ao acesso ao programa de transporte gratuito, caso terceiros utilizassem os dados de forma indevida, limitando o exercício desse benefício.

Além disso, a falta de notificação individual impediu os titulares de adotarem medidas preventivas, agravando as potenciais consequências em termos de privacidade e segurança pessoal.

> ⚠ **Gravidade da infração: grave**
>
> A falta de comunicação individualizada aos titulares foi considerada como um fator que impactou significativamente os direitos e interesses dos afetados pelo incidente, classificando a infração como de gravidade média[19]. A situação se agravou devido à exposição de dados pessoais sensíveis, como o tipo de deficiência e laudos médicos, além de dados referentes a crianças e adolescentes.[20]

19 Regulamento de Dosimetria e Aplicação de Sanções Administrativas. Art. 8º, 2º.

20 Regulamento de Dosimetria e Aplicação de Sanções Administrativas. Art. 8º, §3º, "d"

Sanção aplicada: Advertência com medidas corretivas

Com base no art. 9º, inciso II, do Regulamento de Dosimetria, a sanção de advertência foi considerada apropriada, pois exige a implementação de medidas corretivas. As medidas impostas foram:

- Envio de uma comunicação direta e individualizada a cada titular afetado;
- Atualização e manutenção do comunicado geral sobre o incidente no site por 90 dias.

A ANPD também destacou que, apesar da possibilidade de aplicação de multa simples em casos de infrações graves[21], essa penalidade foi descartada devido ao caráter público da entidade.[22]

(II) FALHA AO IMPLEMENTAR MECANISMOS DE SEGURANÇA ADEQUADOS (ART. 49 DA LGPD)

Foi constatado que a SDSCJ-PE não implementou medidas básicas de segurança para proteger sua base de dados, em violação ao art. 49 da LGPD. As medidas de segurança exigidas não foram seguidas, permitindo o acesso irrestrito a uma planilha contendo dados pessoais diretamente no site da Secretaria, sem qualquer controle de acesso.

Além disso, a SDSCJ-PE não conseguiu esclarecer dois pontos cruciais para a compreensão do incidente, quais sejam:

i. o momento exato em que a violação de segurança começou; e

ii. a vulnerabilidade explorada ou a causa raiz do incidente.

Com base nas evidências, a ANPD concluiu que não havia monitoramento de acesso adequado que explicasse o período em que os dados permaneceram expostos, seja por acesso indevido aos servidores, bases de dados ou aplicações web, falha humana ou outra vulnerabilidade.

A ausência de medidas de segurança apropriadas expôs os dados a possíveis danos significativos, como duplicação e uso indevido por terceiros, o que poderia impedir os usuários de exercerem seu direito de acesso ao programa de gratuidade no transporte intermunicipal. Isso poderia limitar o direito de livre locomoção dos titulares afetados, resultando em potenciais prejuízos materiais.

21 Regulamento de Dosimetria e Aplicação de Sanções Administrativas. Art. 3º, §5º

22 Regulamento de Dosimetria e Aplicação de Sanções Administrativas. Art. 3º, §5º,

Gravidade da infração: grave

A ausência de medidas de segurança adequadas foi considerada como um fator determinante para a concretização do incidente, impactando significativamente os direitos e interesses dos titulares afetados. A infração foi classificada como de gravidade média[23], com um agravante devido à presença de dados pessoais sensíveis e informações de crianças e adolescentes[24].

Sanção aplicada: Advertência com medidas corretivas

Conforme o art. 9º, inciso II, do Regulamento de Dosimetria, a sanção de advertência foi considerada apropriada, com a imposição de medidas corretivas.

A ANPD determinou as seguintes ações:

- Comprovação da implementação de medidas técnicas, incluindo:
  - (i) Mecanismos de monitoramento de tráfego;
  - (ii) Armazenamento adequado dos registros de acesso;
  - (iii) Restrição de acesso ao link contendo a base de dados.
- Apresentação de um cronograma para a implementação dessas medidas.

A decisão completa pode ser acessada neste link.

2.6. PROCESSO Nº00261.001969/2022-41 – Instituto de Assistência Médica ao Servidor Público Estadual do Estado de São Paulo

O presente processo trata da apuração de um incidente de segurança envolvendo o Instituto de Assistência Médica ao Servidor Público Estadual de São Paulo (IAMSPE). O IAMSPE reportou que o incidente, ocorrido em janeiro de 2022, poderia ter afetado 1.489.304 titulares, incluindo beneficiários e dependentes.

23 Regulamento de Dosimetria e Aplicação de Sanções Administrativas. Art. 8º, 2º

24 Regulamento de Dosimetria e Aplicação de Sanções Administrativas. Art. 8º, §3º, "d"

Após a confirmação do incidente, a ANPD solicitou ao instituto que adotasse medidas para corrigir a vulnerabilidade e realizasse uma auditoria no sistema para identificar acessos não autorizados. No entanto, apesar das solicitações, o IAMSPE não comunicou individualmente todos os titulares e publicou um comunicado no site que não atendia aos requisitos da LGPD.

A ANPD considerou insuficiente a comunicação realizada e as justificativas apresentadas. Como resultado, foi recomendado e instaurado um processo administrativo sancionador contra o IAMSPE por descumprimento das determinações da ANPD.

(I) COMUNICAÇÃO DO INCIDENTE AOS TITULARES AFETADOS (ART. 48 DA LGPD)

No caso em análise, foram identificadas falhas na comunicação do incidente de segurança aos beneficiários afetados. A notificação aos titulares foi realizada com três meses de atraso e, ainda assim, de forma incompleta, omitindo informações essenciais exigidas pelo Art. 48 da LGPD, como a descrição dos dados afetados e os riscos decorrentes do incidente.

Além disso, a maior parte das comunicações aos titulares foi feita por e-mail, após dificuldades operacionais na validação dos contatos, o que a ANPD considerou uma forma de comunicação insuficiente. A ANPD entendeu que a falta de notificação em prazo razoável, especialmente quando dados pessoais são expostos em espaços de acesso não controlado, afeta significativamente os interesses e direitos fundamentais dos titulares. Sem essa comunicação, os titulares ficam impedidos de tomar as medidas necessárias para evitar o uso indevido de identidade, proteger-se de fraudes financeiras e mitigar outros possíveis danos decorrentes da exposição dos dados. No caso concreto, os dados expostos aumentam a possibilidade de danos, como ligações indevidas, fraudes em processos de autenticação e validação de identidade em serviços específicos.

Gravidade da infração: grave

A falta de comunicação individualizada aos titulares causou impacto significativo aos direitos e interesses dos afetados, classificando a infração inicialmente como média[25]. No entanto, a gravidade foi majorada pela presença de dados pessoais de crianças e adolescente[26].

Sanção aplicada: Advertência com medidas corretivas

Conforme o art. 9º, inciso II, do Regulamento de Dosimetria, a sanção de advertência foi considerada adequada. Além disso, a ANPD exigiu ajustes na redação do comunicado geral publicado no site, com a exigência de mantê-lo disponível por 90 dias.

25 Regulamento de Dosimetria e Aplicação de Sanções Administrativas. Art. 8º, 2º.

26 Regulamento de Dosimetria e Aplicação de Sanções Administrativas. Art. 8º, §3º, "d"

(II) FALHA AO IMPLEMENTAR MEDIDAS DE SEGURANÇA ADEQUADAS (ART. 49 DA LGPD)

A ANPD concluiu que, embora o IAMSPE não tenha registrado evidências de exploração da vulnerabilidade, isso se deveu à ausência de logs de acesso no momento da denúncia. A investigação revelou que as características técnicas do sistema de informação do IAMSPE permitiam o acesso indiscriminado a dados pessoais.

Apesar de o IAMSPE ter implementado medidas de segurança relevantes, como a criação de um Comitê de Privacidade e um programa de segurança de dados, essas ações foram adotadas apenas após o incidente. Por esse motivo, a ANPD considerou que o IAMSPE violou o art. 49 da LGPD, que exige a adoção de medidas preventivas de segurança.

Nesse contexto, a ANPD entendeu que a falta de medidas de segurança adequadas permitiu o acesso aos dados, expondo os titulares ao risco de roubo de identidade e possíveis fraudes financeiras. Foi constatado um risco significativo de que os direitos e interesses dos titulares sejam afetados, incluindo potenciais danos materiais.

Gravidade da infração: grave

A ausência de implementação de medidas de segurança adequadas foi considerada como um fator que possibilitou a concretização do incidente, impactando significativamente os direitos e interesses dos titulares afetados. A infração foi classificada como de gravidade média[27], sendo agravada pela presença de dados pessoais de crianças, adolescentes e idosos.[28]

Sanção aplicada: Advertência com medidas corretivas

Conforme o art. 9º, inciso II, do Regulamento de Dosimetria, a advertência foi considerada adequada. Ainda, ANPD determinou a comprovação de adoção das medidas indicadas no plano de conformidade sugerido pelo IAMPS.

A decisão completa pode ser acessada neste link.

27 Regulamento de Dosimetria e Aplicação de Sanções Administrativas. Art. 8º, 2º.

28 Regulamento de Dosimetria e Aplicação de Sanções Administrativas. Art. 8º, §3º, "d"

← Voltar ao sumário

3. INSIGHTS: PRINCIPAIS ASPECTOS SOBRE A ATUAÇÃO DA ANPD

A partir da análise de casos recentes, é possível observar padrões e diretrizes que norteiam a atuação da ANPD, bem como compreender como a Autoridade interpreta e aplica os princípios da LGPD.

A seguir, destacam-se alguns dos principais insights relacionados à atuação da ANPD no tratamento de incidentes de segurança, no dever de notificação aos titulares, na implementação de medidas de segurança e no impacto do não fornecimento de informações solicitadas.

3.1. Abordagem Responsiva da ANPD

Os casos analisados revelam a abordagem de regulação responsiva adotada pela ANPD, que prioriza a orientação e a promoção da conformidade antes de aplicar sanções punitivas. A Autoridade frequentemente concede ao controlador a oportunidade de corrigir falhas, fornecendo orientações e solicitando relatórios ou a implementação de medidas corretivas. Somente após o descumprimento dessas determinações a ANPD instaura processos sancionadores. Esse método de atuação evidencia o caráter educativo e preventivo da ANPD, que utiliza sanções como último recurso para assegurar a conformidade com a LGPD.

3.2. Tratamento de Incidentes de Segurança: Comunicação aos Titulares

A ANPD tem adotado uma interpretação rigorosa quanto ao dever de notificação, considerando que a falta de comunicação tempestiva ou o uso de métodos inadequados, como avisos gerais em sites, pode comprometer os direitos dos titulares. Em diversos casos, a ausência de uma comunicação clara e imediata aos titulares afetados foi considerada uma violação direta ao art. 48 da LGPD, mesmo quando o controlador publicou um comunicado geral em seu site.

A ANPD entende que a falha na notificação impede os titulares de adotar medidas preventivas contra fraudes ou uso indevido de seus dados, o que pode resultar em danos materiais e na violação de direitos fundamentais. Isso tem sido a base para classificar a infração como média. Nos casos que envolvem dados pessoais sensíveis ou de crianças, adolescentes ou idosos, a Autoridade agravou a gravidade da infração para alta, o que permite a aplicação de multas pecuniárias para empresas privadas.

3.3. Medidas de Segurança: Importância da gestão de acessos e logs

A ANPD enfatiza a relevância de mecanismos robustos de segurança, especialmente no que se refere à gestão de acessos e ao monitoramento de logs nos sistemas. A falta de controle de acesso e a ausência de registros de logs dificultam a avaliação da extensão dos incidentes e configuram violação ao art. 49 da LGPD. A Autoridade também recomenda a adoção de medidas preventivas de segurança, alinhadas aos princípios de responsabilidade e prevenção, para evitar futuros incidentes.

A LGPD impõe ao controlador o dever de proteger os dados pessoais e de demonstrar a implementação de medidas eficazes para garantir essa proteção. A ausência de registros de acesso é considerada uma falha grave no cumprimento desse dever, conforme o art. 49, que exige a utilização de sistemas que assegurem a segurança e a confidencialidade dos dados pessoais.

A ANPD concluiu que a ausência de medidas de segurança adequadas permitiu a ocorrência de incidentes, resultando em impacto significativo nos direitos e interesses dos titulares. Isso levou à classificação da infração como de gravidade média. Contudo, nos casos envolvendo dados pessoais sensíveis e dados de crianças, adolescentes ou idosos a infração foi classificada como grave, devido ao maior risco e potencial de danos aos titulares.

Um ponto relevante, observado no caso da SES-SC, é a responsabilidade do controlador por falhas de segurança no ambiente do operador. A ANPD reforça que, mesmo em casos de terceirização, o controlador continua responsável por garantir que as medidas de segurança sejam adequadamente implementadas no ambiente do operador.

3.4. não fornecimento de informações solicitadas obstrução à fiscalização

A ausência de fornecimento das informações solicitadas pela ANPD, como relatórios de tratamento de incidentes ou registros de acesso, foi considerada uma forma de obstrução à fiscalização.

A ANPD classifica essa conduta como uma infração grave, conforme previsto no art. 5º do Regulamento de Fiscalização. Nos casos analisados, a falta de cooperação prejudica a capacidade de a Autoridade de avaliar adequadamente o incidente e de determinar as medidas corretivas necessárias, o que leva à aplicação de sanções mais severas.

b/luz

deixa com a gente

Para saber mais, acesse nosso site ou
nos acompanhe nas redes sociais.

baptistaluz.com.br