PRADO VIDIGAL

Privacidade & Digital

INCIDENTES DE SEGURANÇA ENVOLVENDO DADOS PESSOAIS:

O que você precisa saber após as últimas sanções da ANPD

Índice

Apresentação

No mês de outubro de 2023, a Autoridade Nacional de Proteção de Dados (ANPD) aplicou novas sanções por infração à legislação de proteção de dados, dessa vez em face de dois órgãos públicos: o Instituto de Assistência ao Servidor Público Estadual de São Paulo (IAMSPE) e da Secretaria de Estado da Saúde de Santa Catarina (SES/SC).

Em ambos os casos, o contexto de aplicação das sanções está relacionado à ocorrência de incidente de segurança envolvendo dados pessoais.
Nesse sentido, os casos podem trazer direcionamentos sobre a postura que a ANPD espera dos agentes de tratamento diante de incidentes. Assim, a partir das informações divulgadas nos despachos decisórios e nos relatórios de instrução dos casos, preparamos este material com reflexões e ***insights*** sobre as decisões.

1. Entendendo os casos decididos pela ANPD

No Processo Administrativo Sancionador nº 00261.001969/2022-41, foram aplicadas ao órgão público autuado **duas sanções de advertência:**

- **Por infração ao art. 48 da LGPD**, que trata do dever de comunicação da ocorrência de incidente que possa acarretar risco ou dano relevante aos titulares. Nesse caso, a ANPD impôs como medida corretiva o ajuste do comunicado publicado no site do órgão, que deverá permanecer disponível por 90 (noventa) dias corridos; e

- **Por infração ao art. 49 da LGPD**, que trata da segurança dos sistemas utilizados para tratamento de dados pessoais. Nesse sentido, também houve imposição de medida corretiva por meio do cumprimento de ações e cronograma de conformidade.

Por sua vez, no Processo Administrativo Sancionador nº 00261.001886/2022-51, foram aplicadas **quatro sanções de advertência:**

- **Por infração ao art. 38 da LGPD**, que trata da obrigação de apresentação de Relatório de Impacto à Proteção de Dados Pessoais (RIPD) quando requisitado pela ANPD;

- **Por infração ao art. 48 da LGPD**, que dispõe sobre o dever de comunicação da ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Em relação a essa infração, a ANPD impôs como medidas corretivas a disponibilização de comunicado sobre o incidente na primeira página do site do órgão por mais de 90 (noventa) dias, bem como o envio de comunicação individualizada para os titulares que puderem ser identificados.

- **Por infração ao art. 49 da LGPD**, que trata da segurança dos sistemas utilizados para tratamento de dados pessoais; e

- **Por infração ao art. 5º do Regulamento de Fiscalização (Resolução CD/ANPD nº1/2021)**, que estabelece os deveres de cooperação dos agentes de tratamento durante a atividade de fiscalização pela ANPD.

2. Comunicação aos titulares

As sanções impostas pela ANPD denotam a visão da Autoridade acerca da comunicação aos titulares como um componente crucial da resposta a incidentes de segurança envolvendo dados pessoais. Nesse cenário, é fundamental ressaltar a ênfase dada pela ANPD **a três fatores**:

TEMPO DE REALIZAÇÃO DA COMUNICAÇÃO

CONTEÚDO E MEIO UTILIZADO PARA A COMUNICAÇÃO.

REALIZAÇÃO DE COMUNICAÇÃO À INTEGRALIDADE DOS TITULARES AFETADOS PELO INCIDENTE

A importância do tempo na comunicação de incidentes destaca a urgência percebida pela ANPD em informar os titulares de maneira rápida e eficaz.

A imposição de sanções relacionadas à demora na notificação dos titulares ressalta a necessidade de atuação ágil por parte das organizações para garantir que os titulares sejam informados dentro de um período considerado razoável.

PONTO DE ATENÇÃO:
O controlador não deve se preocupar apenas com a mera realização da comunicação, mas também em garantir que o conteúdo aborde todas as informações determinadas pela LGPD e pela ANPD e que o meio utilizado seja adequado para que os titulares afetados tomem ciência da ocorrência do incidente.

Em ambos os casos, a ANPD impôs, como medida corretiva, o ajuste do comunicado publicado no site dos órgãos, delimitando que o comunicado deverá permanecer disponível por 90 (noventa) dias corrido. É interessante notar que a redação de comunicado imposta pela ANPD poderá revelar aos demais agentes de tratamento o conteúdo e a estrutura que a Autoridade espera encontrar em tais comunicações.

Para além da disponibilização de informações sobre (i) resumo e data da ocorrência do incidente; (ii) descrição dos dados pessoais afetados; (iii) riscos e consequências aos titulares de dados; (iv) medidas tomadas pelo controlador e as recomendadas aos titulares para mitigar os efeitos do incidente, se cabíveis; e (v) dados de contato do encarregado do controlador para que os titulares possam solicitar informações adicionais a respeito do incidente, é possível extrair os seguintes ***insights***:

- Possibilidade de apresentação das categorias de dados pessoais envolvidos no incidente (ex.: "dados cadastrais"), não havendo listagem completa das informações pessoais afetadas; e

- A título de esclarecimento sobre as medidas adotadas, a redação da ANPD segue o benchmark, se limitando a informar genericamente que houve adoção de ações preventivas e corretivas.

PONTO DE ATENÇÃO:
Em ambos os casos, a infração ao art. 48 da LGPD foi classificada como grave. No processo nº 00261.001969/2022-41, a classificação da infração foi elevada para grave em razão da presença de dados de crianças e adolescentes, enquanto no processo nº 00261.001886/2022-51, em razão do envolvimento de dados sensíveis (dados de saúde).

2.1 Quando comunicar?

É interessante notar que, nas decisões, a ANPD afirma que o "gatilho" para a realização da comunicação não é a comprovação de que o incidente gera risco ou dano relevante aos titulares, mas a mera possibilidade de que o evento acarrete tal risco.

Nesse sentido, no Relatório de Instrução nº 2/2023 a ANPD aponta que "muito embora a comunicação não decorra especificamente da violação do dever de proteger os dados, e sim da possibilidade de que o incidente possa acarretar risco ou dano relevante aos titulares, uma vez caracterizada essa possibilidade, é incabível o argumento da impossibilidade de demonstrar quais titulares foram afetados ou a proporção em que a vulnerabilidade foi explorada, em razão de falha no dever de proteger dados pessoais, para afastar o dever de comunicar sobre o incidente aos titulares".

Diante deste cenário, é possível extrair o entendimento de que a ANPD não considerará o argumento de que não houve realização da comunicação porque não se sabia se realmente havia risco ou dano relevante para os titulares e quais seriam os titulares afetados pelo evento, o que reforça a necessidade de que os agentes de tratamento adotem controles de segurança que permitam a rápida investigação dos fatos.

2.2 Como comunicar?

No Relatório de Instrução nº 4/2023, a ANPD reiterou a orientação de que, sendo possível identificar os titulares afetados pelo incidente, a comunicação deve ser feita a estes de forma direta e individualizada.

No caso, a ANPD considerou que a publicação de nota informativa sobre o incidente no site do órgão não seria o meio adequado para comunicação dos titulares, visto que a divulgação de comunicado geral poderia seria insuficiente para que o titular pudesse preservar seus direitos e tentar diminuir os possíveis prejuízos causados pelo incidente de segurança. Assim, a autoridade impôs como medida corretiva a realização de comunicação individual aos titulares que puderam ser identificados.

3. Segurança e conformidade dos sistemas

Em ambos os casos, foi constatada infração ao art. 49 da LGPD, que trata da segurança dos sistemas utilizados para tratamento de dados pessoais. Nas duas situações, a infração foi classificada como grave.

De modo geral, a ANPD aponta que é de se esperar que o controlador adote medidas adequadas para a proteção de base de dados pessoais sob sua custódia, especialmente quando envolvem alto volume de dados, titulares de grupos vulneráveis ou dados sensíveis.

É interessante notar que, em um dos casos, a parte investigada alegou que, em sua investigação interna, não foi possível obter acesso aos registros (***logs***) do conteúdo acessado, de modo que não haveria evidências de perda ou alteração da base de dados por ausência de logs.

Diante deste cenário, a ANPD aponta que a "ausência de registros (logs) constitui falha no dever de proteger os dados pessoais sob sua custódia. Não há como o controlador cumprir, ou demonstrar que cumpre, seu dever de protegê-los 'de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer outra forma de tratamento inadequado ou ilícito' sem que saiba quando e por quem são acessados".

PONTO DE ATENÇÃO:
Para a ANPD, a ausência de registro de logs de acesso, por si só, constitui uma falha no dever de proteção de dados. Em outras palavras, o agente não pode se valer da ausência de registro de logs de acesso para afirmar que não há comprovação de exploração das vulnerabilidades.

4. Registro de evidências e cooperação com a ANPD

No processo nº 00261.001886/2022-51, a ANPD requereu ao órgão público a apresentação de relatório técnico do incidente, o qual deveria conter, dentre outras, informações sobre: (i) a apuração dos tipos de dados e do número de titulares afetados pelo incidente, apresentando a metodologia utilizada e a justificativa das premissas adotadas; e (ii) a existência de registros (log) de acesso do servidor afetado.

A ANPD considerou a não apresentação do relatório técnico do incidente como descumprimento do dever de fornecer documentos, dados e informações, o que prejudicou a atividade fiscalizatória. Nesse sentido, a ANPD pontuou que em vista da não apresentação dos documentos requeridos, não foi possível formar juízo de certeza sobre a extensão do incidente de segurança.

O caso reforça a importância de as organizações manterem evidências de todas as ações tomadas antes, durante e após o incidente, visto que, além de atender ao princípio da responsabilização e prestação de contas (art. 6º, X, da LGPD), tais registros poderão ser requisitados pela ANPD em caso de fiscalização.

PONTO DE ATENÇÃO:
A não apresentação de relatório técnico do incidente foi classificada como infração de natureza grave, visto que a ANPD considerou que tal violação configurou obstrução à atividade de fiscalização.

5. Considerações finais PVA

As sanções aplicadas pela ANPD indicam uma atuação minuciosa do órgão em casos de incidentes envolvendo dados pessoais nos quais, aos olhos da Autoridade, o dever de comunicação não esteve bem atendido.

Assim, é essencial que as organizações estejam preparadas para lidar com esses eventos, visto que uma atuação ágil e estratégica pode ser decisiva para mitigar os riscos de violação à legislação de proteção de dados.

Para maiores informações sobre o tema, entre em contato com nosso time.

Material produzido por Prado Vidigal Advogados em dezembro de 2023

Autores(as):
Carolina Giovanini
Luis Fernando Prado
Verônica Marques

PRADO VIDIGAL
Privacidade & Digital

PRADO VIDIGAL

Privacidade & Digital

Fale conosco

pradovidigal.com.br

linkedin.com/company/pradovidigal/

@pradovidigal