

PRESIDÊNCIA DA REPÚBLICA
AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS
Coordenação-Geral de Normatização

Nota Técnica nº 3/2021/CGN/ANPD

Processo nº 00261.000098/2021-67

Assunto: Proposta de realização de Tomada de Subsídios para regulamentação do dever de comunicação de incidentes de segurança, nos termos do § 1º do art. 48 da Lei nº 13.709, de 14 de agosto de 2018.

1. RELATÓRIO

1. O item 6 da agenda regulatória bianual 2021-2022 da Autoridade Nacional de Proteção de Dados (ANPD), aprovada pela Portaria nº 11, de 27 de janeiro de 2021, trata da regulamentação da comunicação de incidentes de segurança, incluindo a especificação do prazo de notificação nos termos do § 1º do art. 48 da Lei nº 13.709, de 14 de agosto de 2018, a Lei Geral de Proteção de Dados Pessoais (LGPD).

2. A Análise de Impacto Regulatório estabelece os mecanismos de participação da sociedade no âmbito da sua atuação, incluindo a tomada de subsídios. Esta consiste em importante instrumento administrativo que visa obter subsídios, informações e dados relevantes para o processo regulatório a partir da escuta dos agentes econômicos, consumidores e demais interessados da sociedade, de forma a identificar e aprimorar os aspectos relevantes à matéria em questão.

3. Nesse sentido, vale salientar que a tomada de subsídios ora proposta se alinha à recomendação constante do manual *Diretrizes gerais e guia orientativo para elaboração de Análise de Impacto Regulatório – AIR* [\[1\]](#) publicado pela Casa Civil da Presidência da República:

A realização de Consultas e Audiências Públicas já é prática comum entre as Agências Reguladoras Federais, que seguem os ritos e procedimentos definidos em lei ou outros normativos próprios sobre o tema, e entre alguns órgãos e entidades da Administração Direta. Entretanto, geralmente esses processos são realizados após já tomada a decisão sobre o tipo de ação a ser implementada, buscando colher contribuições e manifestações sobre a minuta do instrumento de intervenção já elaborado.

A boa prática regulatória recomenda que a consulta e o diálogo com os atores interessados no problema regulatório devem começar o mais cedo possível, ainda nos estágios iniciais da AIR. O objetivo é convidar os atores relevantes a contribuir para melhorar a qualidade da análise que orientará a decisão. Quando envolvidos após já tomada a decisão, a tendência é que estes atores só se debrucem sobre a minuta apresentada, questionando seus dispositivos sem considerar o processo de análise que culminou em sua proposição, mesmo que a AIR seja disponibilizada para consulta junto com o instrumento. [Grifos no original]

4. Após análise das contribuições trazidas na tomada de subsídios, será elaborada e submetida à Consulta Pública minuta com a proposta de regulamentação, acompanhada do Relatório de Análise de Impacto Regulatório.

5. Nessa etapa do processo, pretende-se instaurar uma tomada de subsídios para amparar a expedição de minuta de Resolução Normativa.

6. É o relatório.

2. ANÁLISE

7. No que se refere à segurança e ao sigilo dos dados, conforme disposto na Seção I – Da Segurança e do Sigilo dos Dados, do Capítulo VII – Da Segurança e das Boas Práticas, a LGPD, em seu art. 48, prevê a necessidade de comunicação pelo controlador tanto ao titular dos dados quanto à ANPD sobre a ocorrência de incidente de segurança que possa trazer risco ou dano relevante aos titulares, *in verbis*:

Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

8. Em seguida, a LGPD estabelece os critérios para que essa comunicação seja feita, incluindo os requisitos mínimos e a menção de um prazo razoável e, adiante em sua redação, a lei insere um segundo limite ao dispor quais medidas complementares à comunicação podem ser determinadas pela ANPD conforme a gravidade do incidente.

Art. 48. (...)

§ 1º A comunicação será feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo:

I - a descrição da natureza dos dados pessoais afetados;

II - as informações sobre os titulares envolvidos;

III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;

IV - os riscos relacionados ao incidente;

V - os motivos da demora, no caso de a comunicação não ter sido imediata; e

VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.

§ 2º A autoridade nacional verificará a gravidade do incidente e poderá, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao controlador a adoção de providências, tais como:

I - ampla divulgação do fato em meios de comunicação; e

II - medidas para reverter ou mitigar os efeitos do incidente.

§ 3º No juízo de gravidade do incidente, será avaliada eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis, no âmbito e nos limites técnicos de seus serviços, para terceiros não autorizados a acessá-los.

9. Nesse contexto, é importante que, em conjunto com a sociedade, a ANPD construa limites claros que permitam distinguir incidentes de segurança que possam trazer risco ou dano relevante e que possam demandar providências adicionais daqueles cuja ameaça, se houver, pode ser desconsiderada. Assim, é necessário ponderar sobre quais informações devem constar na comunicação tanto ao titular de dados, que lhe sejam úteis para salvaguarda de seus direitos, quanto à ANPD para avaliar o caso.

10. Outro importante aspecto a ser endereçado são as possíveis classificações de risco do incidente que podem ser adotadas pela ANPD, bem como os critérios para que essa classificação seja feita e as eventuais exceções em relação à obrigatoriedade de informar tanto os titulares quanto a Autoridade.

11. Além disso, um importante ponto de discussão diz respeito à regulamentação do prazo razoável para que as empresas informem tanto a ANPD quanto os titulares de dados pessoais sobre os vazamentos de dados. No âmbito da União Europeia, por exemplo, o Regulamento Geral sobre a Proteção de Dados estabelece o prazo de 72h (art. 33, 1) para a notificação da autoridade de controle e prevê que a comunicação ao titular dos dados seja efetuada “sem demora injustificada” (art. 34, 1). Por sua vez, o Decreto nº 9.936, de 24 de julho de 2019, que regulamenta a Lei do Cadastro Positivo, determina que a comunicação à ANPD seja efetuada no prazo de dois dias úteis, contado da data do conhecimento do incidente, prevendo, ainda, “a pronta comunicação aos cadastrados afetados pelo incidente de segurança” (art. 18, I e §§ 1º e 2º).

12. Assim, é relevante considerar se a regulamentação a ser editada pela ANPD deve seguir os parâmetros internacionais e nacionais vigentes ou se seria mais adequado estabelecer regramento diferenciado. De outro lado, questiona-se quais informações adicionais podem ser solicitadas além das que estão previstas nos incisos do §1º do art. 48.

13. As possíveis providências, incluindo medidas técnicas e administrativas que poderão ser determinadas pela ANPD aos controladores após a comunicação do incidente de segurança também devem ser objeto da tomada de subsídios, assim como eventuais metodologias sobre a análise da gravidade do incidente.

14. Assim, por meio desta tomada de subsídios, pretende-se endereçar esses e outros aspectos que se relacionam diretamente à regulamentação da comunicação de incidentes de segurança.

3. CONCLUSÃO

15. Tendo em vista que o tema está previsto na fase 1 de regulamentação na Agenda Regulatória 2021-2022, a tomada de subsídios contribuirá substancialmente para a absorção pela ANPD das distintas abordagens da sociedade sobre tema e, conseqüentemente, para a elaboração da primeira minuta de regulamentação.

16. Diante do exposto, propõe-se a realização de tomada de subsídios da sociedade por meio de intercâmbio documental, com prazo de contribuição de 30 dias a contar da publicação do aviso da tomada de subsídios no sítio eletrônico da ANPD, para obter contribuições para elaboração de minuta de normativo e análise de impacto regulatório.

17. À consideração superior.

Rodrigo Santana dos Santos

Coordenador de Normatização

Fabricio Guimarães Madruga Lopes

Coordenador de Normatização

18. De acordo.

Isabela Maiolino

Coordenadora-Geral de Normatização

[1] BRASIL. Casa Civil. Presidência da República (org.). **Diretrizes gerais e guia orientativo para elaboração de Análise de Impacto Regulatório – AIR**. 2018. Disponível em: https://www.gov.br/casacivil/pt-br/centrais-de-conteudo/downloads/diretrizes-gerais-e-guia-orientativo_final_27-09-2018.pdf/view. Acesso em: 18 fev. 2021.



Documento assinado eletronicamente por **Isabela Maiolino, Coordenadora-Geral de Normatização**, em 22/02/2021, às 09:38, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



Documento assinado eletronicamente por **Fabricio Guimarães Madruga Lopes, Coordenador(a)**, em 22/02/2021, às 09:40, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



Documento assinado eletronicamente por **Rodrigo Santana dos Santos, Coordenador(a)**, em 22/02/2021, às 09:53, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



A autenticidade do documento pode ser conferida informando o código verificador **2398694** e o código CRC **7F352A97** no site:

https://super.presidencia.gov.br/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0