00261.000098/2021-67

Presidência da República
AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS
Coordenação-Geral de Normatização

Nota Técnica nº 36/2022/CGN/ANPD

Assunto: **Encaminhamento da minuta de Regulamento de comunicação de incidente de segurança com dados pessoais à Procuradoria da Autoridade Nacional de Proteção de Dados.**

Referência: processo nº 00261.000098/2021-67

1. **RELATÓRIO**

1.1. Trata-se de proposta de Regulamento de comunicação de incidente de segurança com dados pessoais, que tem por objetivo a 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).

1.2. O referido tema encontra-se previsto no item 6 da Agenda Regulatória da Autoridade Nacional de Proteção de Dados (ANPD) para o biênio 2021/2022, aprovada pela Portaria nº 11, de 27 de janeiro de 2021.

1.3. O processo de regulamentação teve início por meio de assinatura de Termo de Abertura de Projeto em 22 de fevereiro de 2021 e conta com os seguintes integrantes em sua equipe de projeto: Fabrício Guimarães Madruga Lopes/CGN e Rodrigo Santana dos Santos/CGN, além de outros servidores indicados posteriormente.

1.4. Diante da complexidade do tema, optou-se pela realização de Tomada de Subsídios por meio do recebimento de contribuições escritas nos termos da Nota Técnica n° 3/2021/CGN/ANPD (SEI 2398694), de modo a possibilitar a participação da sociedade acerca de questões relacionadas à comunicação de incidentes de segurança. Nesse sentido, foram disponibilizadas 13 (treze) perguntas (SEI 2398738) à sociedade, sobre as quais esta Coordenação-Geral de Normatização (CGN) recebeu as respostas no período de 22/02/2021 e 24/03/2021.

1.5. Além disso, entre os dias 15 e 18/03/2022, foram realizadas Reuniões Técnicas com representantes do Núcleo de Informação e Coordenação do Ponto BR (NIC.br), Centro de Direito, Internet e Sociedade (CEDIS) e Instituto Brasileiro de Defesa do Consumidor (IDEC) (SEI nº 2474721); representantes do Laboratório de Políticas Públicas e Internet (LAPIN) e Instituto de Referência em Internet e Sociedade (IRIS-BH) (SEI nº 2475226); representantes do Instituto de Pesquisa em Direito e Tecnologia do Recife (IP.REC) e Coding Rights (SEI nº 2475382); representantes do Data Privacy Brasil e Privacy Academy (SEI nº 2475465) e representantes do ITS Rio e Internet Lab (SEI nº 2483002).

1.6. Após análise das 98 (noventa e oito contribuições) recebidas durante a tomada de subsídios e das discussões realizadas no âmbito das reuniões técnicas, elaborou-se, no âmbito da equipe de projeto, a primeira versão da minuta, que foi submetida a consulta interna de 08 a 29 de julho de 2022 (SEI nº 3616715).

1.7. Feita a análise das contribuições internas, a minuta foi ajustada e debatida com o Conselho Diretor por meio de Seminário Interno dividido em quatro reuniões, realizado nos dias 28 de julho de 2022, e em 2, 4 e 12 de agosto do mesmo ano (SEI nº 3616751, 3616753, 3616757 e 3616768).

1.8. Após a realização de ajustes na minuta, resultado da discussão com o Conselho Diretor, a presente minuta com a proposta de regulamentação, devidamente acompanhada do Relatório de Análise de Impacto Regulatório (AIR), segue para avaliação da Procuradoria da ANPD. Na sequência, o processo será enviado ao Conselho Diretor para deliberação da matéria e autorização de submissão da proposta normativa à consulta pública.

1.9. É o relatório.

2. **ANÁLISE**

2.1. **Da fundamentação legal**

2.1.1. Incialmente, cumpre destacar que em fevereiro de 2022, a Emenda Constitucional nº 115, de 2022 alçou o direito à proteção de dados pessoais, para o rol dos direitos e garantias fundamentais, além de ter fixado a competência privativa da União para legislar sobre o tema.

2.1.2. De fato, a LGPD inaugurou um novo regime jurídico referente ao tratamento de dados pessoais no país, conferindo prerrogativas à ANPD para zelar, implementar e fiscalizar o cumprimento da lei em todo o território nacional. Desta forma, a ANPD é a autarquia federal responsável por dar efetividade à LGPD no País.

2.1.3. Entre as competências da ANPD, consta o estabelecimento de normas e diretrizes para a interpretação e implementação da LGPD. Para além da competência normativa, a LGPD também atribuiu à ANPD a competência fiscalizatória e sancionatória em matéria de tratamento de dados pessoais, prevalecendo, no que se refere à proteção de dados pessoais, sobre as competências correlatas de outras entidades ou órgãos da administração pública, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito ao recurso, *in verbis* (grifo nosso):

> Art. 55-J. Compete à ANPD:
>
> (...)
>
> XIII - **editar regulamentos** e procedimentos sobre proteção de dados pessoais e privacidade, bem como sobre relatórios de impacto à proteção de dados pessoais para os casos em que o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos nesta Lei; (Incluído pela Lei nº 13.853, de 2019)

2.1.4. Ademais, destaca-se que o Regimento Interno da ANPD (RIANPD), aprovado pela Portaria nº 1, de 8 de março de 2021, em seu art. 16, atribuiu a esta Coordenação-Geral de Normatização (CGN) as competências de elaboração de guias e recomendações, bem como proposições normativas, regulamentos, orientações e procedimentos simplificados, nos termos da LGPD, a serem submetidas à aprovação pelo Conselho Diretor.

2.1.5. No tocante ao objeto de regulamentação, o art. 48 da LGPD ao prever que 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, determinou, em seu §1º que tal comunicação deverá ser realizada em prazo razoável, a ser definido pela Autoridade, e estabeleceu requisitos mínimos para que a mesma fosse realizada:

> 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.
>
> § 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.