Autoridade Nacional de Proteção de Dados
Coordenação-Geral de Normatização
Nota Técnica nº 92/2023/CGN/ANPD

Processo nº 00261.000098/201-67

Interessado: Procuradoria Federal Especializada - PFE/ANPD

Assunto: **Análise das contribuições da Consulta Pública referente à proposta de Regulamento de Comunicação de Incidente de Segurança com Dados Pessoais (RCIS).**

Referência: Processo nº 00261.000098/2021-67

1. RELATÓRIO

1. Em fevereiro de 2021, esta Coordenação-Geral de Normatização (CGN) iniciou, por meio do Termo de Abertura de Projeto (TAP) (SEI nº 2388029), o presente processo para elaboração de ato normativo para regulamentar o procedimento de notificação de incidentes de segurança, nos termos do disposto no artigo 48 da Lei nº 13.709, de 14 de agosto de 2018, a Lei Geral de Proteção de Dados Pessoais (LGPD), com vistas a instrumentalizar o exercício da competência fiscalizatória da ANPD, e atender ao item 6 da Agenda Regulatória para o biênio 2021-2022, aprovada pela Portaria nº 11, de 27 de janeiro de 2021, que passou a ser o item 3 da Agenda Regulatória para o biênio 2023-2024, aprovada pela Portaria ANPD nº 35, de 4 de novembro de 2022.

2. Com o fito de obter insumos para o processo de regulamentação, 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 nº 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 nº 2398738) à sociedade, sobre as quais esta Coordenação-Geral recebeu as respostas no período de 22/02/2021 e 24/03/2021.

3. Além disso, entre os dias 15 e 18 de março de2022, 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* (2483002).

4. 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, conforme Certidão nº 9 (SEI nº 3616715).

5. Feita a análise das contribuições internas, a minuta foi ajustada e debatida com o Conselho Diretor por meio de Seminário Interno dividido em 4 (quatro reuniões), realizadas 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).

6. Ato contínuo, a proposta de regulamentação, devidamente acompanhada do relatório de Análise de Impacto Regulatório (AIR), seguiu para avaliação da Procuradoria Federal Especializada (PFE) da ANPD em 16 de setembro de 2022, mediante a Nota Técnica nº 36/2022/CGN/ANPD (SEI nº 3632102).

7. Em 19 de dezembro de 2022, a PFE/ANPD se manifestou por meio do Parecer nº 00023/2022/GAB/PFE-ANPD/PGF/AGU (SEI nº 3819738), em atendimento ao parágrafo único do art. 50 do Regimento Interno da ANPD, aprovado pela Portaria nº 1, de 8 de março de 2021 (RIANPD).

8. As recomendações da PFE/ANPD foram analisadas por meio da Nota Técnica nº 12/2023/CGN/ANPD (SEI nº 4012432), que encaminhou o processo à Secretaria Geral da ANPD, junto com uma nova versão da minuta de resolução (SEI nº 4013386).

9. Em 26 de abril de 2023, o Conselho Diretor da ANPD aprovou a submissão da minuta de resolução a Consulta Pública, nos termos do art. 53 da LGPD, conforme a Ata de Circuito Deliberativo do Conselho Diretor nº 9 (SEI nº 4192688).

10. Assim, nos termos do Documento Consulta Pública nº 1/2023 DOU (SEI nº 4205815), de 27 de abril de 2023, a minuta de resolução foi submetida à Consulta Pública, com prazo de 30 (trinta) dias para envio de sugestões, entre os dias 02 e 31 de maio de 2023.

11. Por meio do Aviso Audiência Pública Nº 1/2023 DOU (SEI nº 4213493), publicado em DOU de 04 de maio de 2023, o Conselho Diretor da ANPD determinou a realização de Audiência Pública, prevista no art. 55-J, § 2º, da LGPD, destinada ao debate e manifestação da sociedade sobre a minuta de resolução, realizada no dia 23 de maio de 2023, disponível em https://www.youtube.com/watch?v=5KCIVpnmnsA&ab_channel=anpdgov.

12. Em 31 de maio de 2023, conforme Despacho DOU (SEI nº 4298880), o Conselho Diretor da ANPD prorrogou o prazo de realização da consulta pública sobre o Regulamento de Comunicação de Incidente de Segurança com Dados Pessoais por 15 (quinze) dias.

13. Foram recebidas, pela plataforma Participa + Brasil, 1.491 (mil quatrocentos e noventa e uma) contribuições de 103 (cento e três) participantes no âmbito da consulta pública, além de ouvidas 47 (quarenta e sete) pessoas na Audiência Pública.

14. É o Relatório.

2. ANÁLISE

Da contribuições recebidas na Consulta Pública:

15. O §2º do art. 55-J da LGPD estabelece que a ANPD realize consulta e audiência pública antes de publicar os seus atos normativos, permitindo, assim, a promoção do diálogo direto entre a Autoridade e o cidadão no processo de regulamentação da proteção de dados pessoais no Brasil.

16. Já o art. 62 do Regimento Interno da ANPD, aprovado pela Portaria nº 1, de 8 de março de 2021, prevê que a consulta pública deve ser formalizada por publicação no Diário Oficial da União, com prazo não inferior a dez dias, devendo as críticas e as sugestões serem apresentadas conforme dispuser o respectivo instrumento deliberativo.

17. Assim, em atenção aos normativos mencionados, por meio do Documento Consulta Pública nº 1/2023 DOU (SEI nº 4205815), de 27 de abril de 2023, a minuta de resolução foi submetida a consulta pública, pelo prazo de trinta dias, para envio de sugestões, entre os dias 02 e 31 de maio de 2023.

18. Em 31 de maio de 2023, conforme Despacho DOU (SEI nº 4298880), o Conselho Diretor da ANPD prorrogou o prazo de realização da consulta pública sobre o Regulamento de Comunicação de Incidente de Segurança com Dados Pessoais por quinze dias.

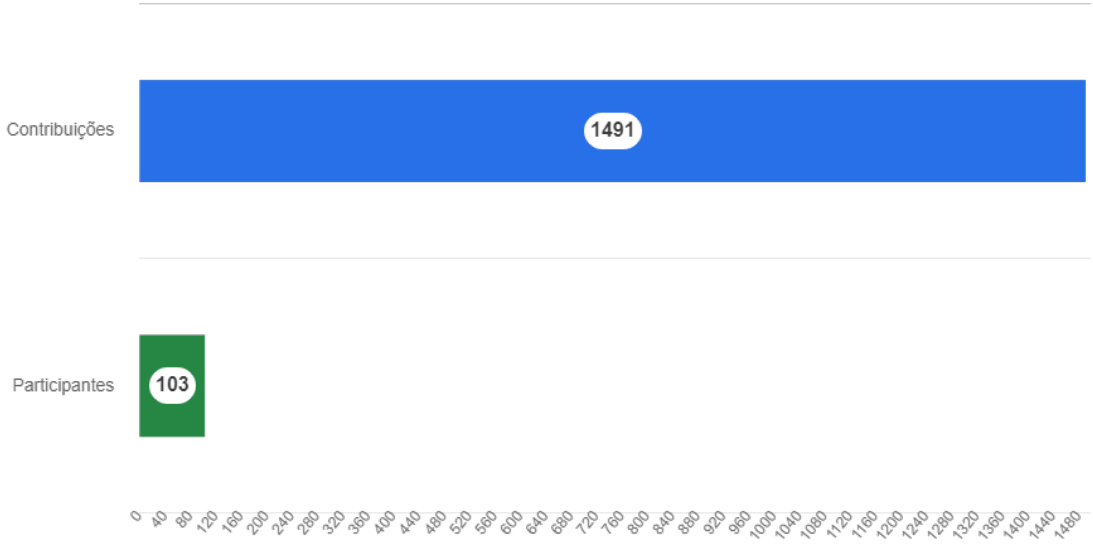
19. Sobre ambas as ocasiões, houve divulgação na página da ANPD na Internet após sua publicação no Diário Oficial da União, em atendimento ao § 2º do art. 62 do Regimento Interno.

20. Segundo o Despacho supracitado, as críticas e sugestões deveriam ser formalmente encaminhadas e devidamente justificadas para apreciação da Autoridade quando da elaboração da proposta final de ato normativo.

21. A consulta esteve disponível na plataforma Participa + Brasil[1]

pelo prazo estipulado e foram recebidas 1.491 (mil quatrocentos e noventa e uma) contribuições de 103 (cento e três) participantes na consulta pública, conforme pode ser observado no gráfico abaixo e consultado na planilha (SEI nº 4842720).

Gráfico 1 - Quantidade de Contribuições e Participantes na Consulta Pública

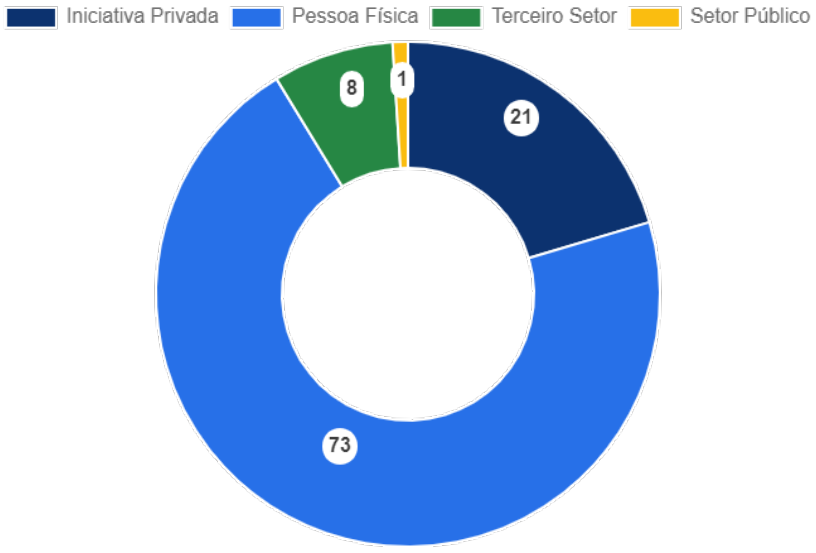


Fonte: Plataforma Participa + Brasil

22. Quanto aos participantes, 73 (setenta e três) são pessoas naturais, 21 (vinte e um) representam a iniciativa privada, 8 (oito) são do terceiro setor e 1 (um) representante é proveniente do setor público.

23. Deve-se salientar que as contribuições relativas às pessoas naturais podem ter sido submetidas em nome de empresas da iniciativa privada, do setor público ou terceiro setor.

Gráfico 2 - Perfil dos Participantes na Consulta Pública



Fonte: Elaboração da equipe da CGN

24. Quanto à distribuição da participação social por Unidades da Federação (UF), 809 (oitocentos e nove) contribuições foram do Estado de São Paulo, UF com maior representatividade, sendo de 54,3%, seguida pelo Rio de Janeiro com 246 (duzentas e quarenta e seis) contribuições, equivalente a 16,5% do total. Do Distrito Federal foram apresentadas 104 (cento e quatro) contribuições, o que representa 7% da totalidade.

25. Outras UFs que tiveram representatividade foram Minas Gerais (2%), Santa Catarina (1,8%), Paraná (1,4%), Rio Grande do Sul (0,3%) e Ceará (0,1%).

26. Da análise dos dados, conclui-se que a participação social foi concentrada nas UFs das regiões Sul e Sudeste do Brasil além do Distrito Federal. Cabe destacar a ausência de participação na Consulta Pública das UFs da região Norte e a baixa representatividade da região Nordeste.

27. A CGN analisou todas as contribuições para fins de admissibilidade, objetivando não publicizar aquelas de conteúdo não conexo ou irrelevante para a matéria em análise.

28. Assim, do total de contribuições recebidas, 1.480 (mil quatrocentos e oitenta) foram admitidas para publicização e posterior análise de mérito pela equipe de projeto. As outras 11 (onze) contribuições não foram aprovadas por terem sido decorrentes de duplicidades.

29. Todas as contribuições admitidas foram consideradas na análise realizada pela equipe de projeto, que é composta por servidores de diversas áreas da ANPD[2] , e analisadas por conexão, tendo sido eliminadas as repetitivas, em conformidade com o § 6º do art. 62, do Regimento Interno da ANPD.

30. A seguir, serão apresentadas as contribuições recebidas em grupos, bem como a nova redação sugerida pela Equipe de Projeto após a análise das contribuições recebidas na consulta pública e na audiência pública.

Das Contribuições recebidas na Audiência Pública:

31. Durante a Audiência Pública, realizada em 23 de maio de 2023, foram recebidas contribuições de 47 (quarenta e sete) pessoas. As contribuições orais foram analisadas conjuntamente com aquelas recebidas durante a consulta pública.

32. A mídia da audiência pública está disponível no canal da ANPD no YouTube.[3]

Análise das Contribuições:

33. As contribuições efetuadas, além de apresentarem propostas no intuito de conferir maior clareza ao texto, sugeriram a inclusão de novos dispositivos e a exclusão de outros já existentes na minuta de regulamento.

34. Para melhor compreensão, a seguir serão analisadas as contribuições apresentadas e agrupadas por conexão ao tema ao qual se referem, consoante previsão no art. 62, § 6º, do Regimento Interno da ANPD.

35. As referências aos números de artigos referem-se à versão submetida à consulta pública, exceto quando mencionado de maneira diversa.

36. Após a análise das contribuições, é apresentada a nova proposta redacional, sendo que as redações suprimidas se encontram tachadas e as inseridas em negrito, para melhor compreensão da proposta.

Resolução:

37. A minuta de resolução colocada em consulta pública tem o seguinte texto para esta seção:

RESOLUÇÃO CD/ANPD Nº X, DE XX DE XXXXXXXXXX DE 2023

Aprova o Regulamento de Comunicação de Incidente de Segurança com Dados Pessoais.

O CONSELHO DIRETOR DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD), com base nas competências previstas no art. 55-J, inciso XIII, da Lei nº 13.709, de 14 de agosto de 2018, no art. 2º, inciso XIII, do Anexo I do Decreto nº 10.474, de 26 de agosto de 2020, no art. 5º, inciso I do Regimento Interno da Autoridade Nacional de Proteção de Dados (ANPD), aprovado pela Portaria nº 1, de 8 de março de 2021,

CONSIDERANDO o que consta nos autos do Processo nº 00261.000098/2021-67; e

CONSIDERANDO a deliberação tomada no Circuito Deliberativo nº XX/2023, resolve:

Art. 1º Aprovar o Regulamento de Comunicação de Incidente de Segurança com Dados Pessoais na forma do anexo desta Resolução.

Art. 2º O inciso II do art. 14 do Regulamento de aplicação da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), para agentes de tratamento de pequeno porte, aprovado pela Resolução CD/ANPD nº 2, de 27 de janeiro de 2022, passa a vigorar com a seguinte redação:

"Art. 14.....

II - na comunicação à ANPD e ao titular da ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares, prevista no caput dos arts. 6º e 9º do Regulamento de Comunicação

de Incidente de Segurança com Dados Pessoais, aprovado pela Resolução CD/ANPD nº X, de XX de XXXXXXX de 2023.” (NR)

Art. 3º Esta Resolução entra em vigor em 1º de xxxxxx de 2023.

Contribuições recebidas:

38. Das contribuições apresentadas para este capítulo, destacam-se, pela relevância, as sugestões descritas abaixo.

39. Em relação ao preâmbulo da minuta deResolução, foram recebidas 2 (duas) propostas de inclusão do inciso XVI do art. 55-J da Lei nº 13.709, de 2018, a Lei Geral de Proteção de Dados Pessoais (LGPD), respeitante à competência para realizar auditorias, ou determinar sua realização, no âmbito da atividade de fiscalização, no rol de dispositivos que relacionados às competências que fundamentam a edição do ato normativo.

40. Relativamente ao art. 2º da minuta deResolução, houve 1 (uma) proposição para alteração da Resolução CD/ANPD nº 4/2022 nos seguintes termos:

"(...) para que o processo de comunicação atinja seus propósitos, ou seja, para que haja o incentivo entre as duas partes para a resolução de incidentes de segurança, sugere-se a alteração no art. 13, III, a, e § 1º, da Resolução CD/ANPD nº 4/2022, para que a aplicação da redução de 20% de multa também se aplique para aquelas medidas implementadas no âmbito do processo de comunicação de incidente de segurança, bem como para que se ressalve as providências e medidas mitigadoras determinadas em processo de comunicação de incidente de segurança na hipótese do § 1º adicionando:

Art. Xº - O inciso III, alínea “a” do art. 13 e seu § 1º, do Regulamento de Dosimetria e Aplicação de Sanções Administrativas, aprovado pela Resolução CD/ANPD nº 4, de 24 de fevereiro de 2022, passa a vigorar com a seguinte redação: Art. 13.....

III - nos casos em que o infrator tenha comprovado a implementação de medidas capazes de reverter ou mitigar os efeitos da infração sobre os titulares de dados pessoais afetados:

a) 20% (vinte por cento), previamente à instauração de procedimento preparatório ou processo administrativo sancionador pela ANPD ou no âmbito do processo de comunicação de incidente de segurança com dados pessoais; ou

b) 10% (dez por cento), se após a instauração de procedimento preparatório e até a instauração de processo administrativo sancionador; e

IV - 5% (cinco por cento), nos casos em que se verifique a cooperação ou boa-fé por parte do infrator.”

41. Por fim, no que tange ao art. 3º da minuta deResolução, foram 6 (seis) contribuições relativas a vacatio legis, dentre as quais foram propostos prazos de 3 (três), 6 (seis) e 12 (doze) meses para a entrada em vigor do ato normativo.

Análise:

42. A equipe de projeto entende pela desnecessidade de se incluir o inciso XVI do artigo 55-J da LGPD no preâmbulo da minuta de Resolução, pois a competência para editar regulamentos e procedimentos sobre proteção de dados pessoais e privacidade encontra-se previsto no inciso XIII desse mesmo artigo e a função fiscalizatória não é fundamento para edição de ato normativo.

43. Relativamente à contribuição concernente ao art. 2º daminuta de Resolução, não se vislumbra necessidade de mudança na redação para registrar alteração na norma de dosimetria (Resolução CD/ANPD nº 4/2022), haja vista que há o pressuposto de aplicação do art. 13, III, "a", e § 1º da referida norma no âmbito de infrações relacionadas a incidente de segurança.

44. Quanto ao prazo de vacatio legis, ressalte-se que a primeira versão da minuta de resolução prescrevia a sua entrada em vigor na data da publicação, modificando-a após recomendação da Procuradoria Federal Especializada da ANPD no âmbito do Parecer nº 00023/2022/GAB-PFE/AGU (3819738), a fim de que a vacatio legis estivesse em acordo com a previsão do art. 4º do Decreto nº 10.139, de 28 de novembro de 2019, infra:

> Art. 4º Os atos normativos estabelecerão data certa para a sua entrada em vigor e para a sua produção de efeitos:
> I - de, no mínimo, uma semana após a data de sua publicação;
> e II - sempre no primeiro dia do mês ou em seu primeiro dia útil.
> Parágrafo único. O disposto neste artigo não se aplica às hipóteses de urgência justificada no expediente administrativo.

45. A entrada em vigor do Regulamento, malgrado possa ser firmada com base nos critérios de conveniência e oportunidade do Conselho Diretor da ANPD, entende-se que os agentes de tratamento necessitarão de um período de adaptação, especialmente para organização dos documentos e obrigações previstos no regulamento.

46. Nesse sentido, sugere-se que o art. 3º disponha que a Resolução passe a entrar em vigor no 1º dia útil do terceiro mês subsequente à sua publicação.

Proposta de nova redação para os dispositivos em pauta:

47. Após a análise das contribuições acima citadas, bem como em razão do que dispõe as alíneas "b" e "c" do inciso VI do art. 17 do Decreto nº 9.191, de 1º de novembro de 2017, a seguir, apresenta-se nova proposta:

RESOLUÇÃO CD/ANPS Nº X, DE XX DE XXXXXXXXX DE XXXX

Aprova do Regulamento de Comunicação de Incidente de Segurança com dados pessoais

O CONSELHO DIRETOR DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD), com base nas competências previstas no art. 55-J, inciso XIII, da Lei nº 13.709, de 14 de agosto de 2018, no art. 2º, inciso XIII, do Anexo I do Decreto nº 10.474, de 26 de agosto de 2020, no art. 5º, inciso I do Regimento Interno da Autoridade Nacional de Proteção de Dados (ANPD), aprovado pela Portaria nº 1, de 8 de março de 2021,

CONSIDERANDO o que consta nos autos do Processo nº 00261.000098/2021-67; e

CONSIDERANDO a deliberação tomada no Circuito Deliberativo nº XX/2023, resolve:

Art. 1º Aprovar o Regulamento de Comunicação de Incidente de Segurança com Dados Pessoais na forma do anexo desta Resolução.

Art. 2º O inciso II do art. 14 do Regulamento de aplicação da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), para agentes de tratamento de pequeno porte, aprovado pela Resolução CD/ANPD nº 2, de 27 de janeiro de 2022, passa a vigorar com a seguinte redação:

"Art. 14.

.....

.....

II - na comunicação à ANPD e ao titular da ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares, prevista no *caput* dos arts. 6º e 9º do Regulamento de Comunicação de Incidente de Segurança com Dados Pessoais, aprovado pela Resolução CD/ANPD nº X, de XX de XXXXXXX de 2023**;**

....." (NR)

Art. 3º Esta Resolução entra em vigor em 1º de xxxxxx de 2023.

Regulamento (Anexo à Resolução) Cap. I - Das Disposições Preliminares:

48. A minuta do regulamento colocada em consulta pública tem o seguinte texto para esta seção:

CAPÍTULO I

DAS DISPOSIÇÕES PRELIMINARES

Art. 1º Este Regulamento tem por objetivo normatizar o processo de comunicação de incidente de segurança com dados pessoais que possa acarretar risco ou dano relevante aos titulares, nos termos do art. 48 da Lei nº 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD).

> Art. 2º O processo de comunicação de incidente de segurança com dados pessoais atenderá aos seguintes objetivos:
>
> I - proteger os direitos dos titulares;
>
> II - assegurar a adoção das medidas necessárias para mitigar ou reverter os efeitos dos prejuízos gerados;
>
> III - incentivar o princípio da responsabilização e da prestação de contas pelos agentes de tratamento;
>
> IV - promover a adoção de regras de boas práticas e de governança e de medidas de prevenção e segurança adequadas;
>
> V - estimular a promoção da cultura de proteção de dados pessoais;
>
> VI - garantir que os agentes de tratamento atuem de forma transparente, e estabeleçam uma relação de confiança com o titular; e
>
> VII - fornecer subsídios para as atividades regulatórias, de fiscalização e sancionadora da Autoridade Nacional de Proteção de Dados (ANPD).

Contribuições recebidas:

49. Das contribuições apresentadas para este capítulo, destacam-se, pela relevância, as sugestões descritas abaixo.

50. A fim de alterar o enunciado do objeto e a indicação do âmbito de aplicação do Regulamento, foi sugerido acrescer parte final ao art. 1º, a seguir:

> "(...) art. 48 da Lei nº 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD), bem como incentivar a resolução de incidentes por meio de medidas adequadas de mitigação dos riscos e assecuratórias aos titulares envolvidos e condutas colaborativas entre os agentes de tratamento, os titulares e a ANPD."

51. Além disso, sugeriu-se incluir parágrafo único ao art. 1°:

> "(...) Parágrafo único. Todos os procedimentos elencados neste Regulamento serão iniciados nos termos de atividades de orientação e atividades preventivas, conforme Capítulos III e IV do Título II da Resolução CD/ANPD Nº 1, de 28 de outubro de 2021, que aprova o Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador no âmbito da Autoridade Nacional de Proteção de Dados, exceto quando explicitamente ind.

52. No que tange ao art. 2º, 5 (cinco) contribuições propuseram ajustes no inciso II, para inclusão dos seguintes termos destacados em negrito:

> "(...) II - assegurar
>
> a adoção das medidas necessárias para mitigar ou reverter os efeitos, na **hipótese** de prejuízos **comprovadamente** gerados."
>
> "(...) II - assegurar a adoção das medidas necessárias para mitigar ou

reverter os efeitos, **no caso** de prejuízos gerados;"

"(...) II - assegurar a adoção das medidas necessárias para mitigar ou reverter os efeitos, **na hipótese** de prejuízos gerados"

"(...) II - assegurar a adoção das medidas necessárias para **evitar**, mitigar ou reverter os efeitos **adversos** dos prejuízos gerados;

53. Houve 2 (duas) contribuições a fim de ajustar a redação do inciso III, para que, no lugar de incentivar, constasse assegurar a efetividade.]

54. Ademais, 1 (uma) contribuição sugeriu inclusão de termos no inciso V para constar a seguinte redação: "(...) V - estimular a promoção da cultura de proteção de dados pessoais, com enfoque na conscientização dos agentes de tratamento e na promoção de ações e publicações educativas;

55. Igualmente, 2 (duas) contribuições sugeriram exclusão de termos "fiscalização e sancionadora" no inciso VII, passando-se à seguinte redação: "(...) VII - fornecer subsídios para as atividades regulatórias da Autoridade Nacional de Proteção de Dados" (ANPD).

56. Ainda quanto ao art. 2º, 1 (uma) contribuição sugeriu a inclusão de parágrafo único para prever o sigilo como regra no âmbito do processo de comunicação de incidentes e a necessidade de respeito aos segredos comercial e industrial, da seguinte forma: "Parágrafo único. O processo de comunicação de incidente de segurança correrá em sigilo, observados os segredos comercial e industrial".

Análise:

57. O art. 1º do anexo da minuta de Resolução deve estatuir a finalidade do Regulamento, isto é, dispor de normas a serem obedecidas no âmbito da comunicação de incidente de segurança com dados pessoais que possa acarretar risco ou dano relevante aos titulares, em consonância com o art. 7º da Lei complementar nº 95, de 1998. Por essa razão, a equipe de projeto não atendeu aos pedidos de inclusão de texto no caput desse artigo e de parágrafo único.

58. Quanto à contribuição para o inciso II no art. 2º, a Equipe de Projeto também entendeu ser desnecessária, uma vez que o inciso VI do § 1º do art. 48 da LGPD indica que a comunicação deverá mencionar as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo. A redação minutada apenas parafraseou o texto da lei de forma a conformá-lo à expressão de um objetivo, explicitando, ao final, que os prejuízos são aqueles gerados pelo incidente.

59. Para o inciso III, a equipe de projeto concordou com o ajuste de redação, para que, no lugar de incentivar, conste assegurar a efetividade, pois a comunicação de incidente de segurança não tem como finalidade incentivar a demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados

pessoais e, inclusive, da eficácia dessas medidas, conforme trata a definição inscrita no inciso X do art. 6º da LGPD, mas de garantir ou assegurar a efetividade da prática desse ato de demonstração.

60. Em relação às contribuições quanto aos incisos V e VII, recorda-se que a regulamentação decorre do art. 48 da LGPD. Não é seu objetivo dar enfoque sobre ações educativas ou conscientização de agente de tratamento ao se promover a cultura de proteção de dados pessoais, mas fiscalizar as ações relacionadas à proteção de dados pessoais em situações de incidente de segurança. Daí, é, por natureza, procedimento fiscalizatório capaz de subsidiar as atividades de regulação, de fiscalização e de aplicação de penalidade da ANPD.

61. Por fim, quanto à sugestão de inclusão de parágrafo único para prever o sigilo como regra no âmbito do processo de comunicação de incidentes e a necessidade de respeito aos segredos comercial e industrial, a equipe de projeto entendeu inadequada em virtude de a ANPD atuar em conformidade com o princípio da transparência, conforme disposto no art. 6º, VI da LGPD.

Proposta de nova redação para os dispositivos em pauta:

62. Após a análise das contribuições acima citadas, apresenta-se a nova proposta de redação, incluindo-se ajustes de ofício, pela equipe de projeto, nos caputs do art. 1º e do art. 2º, a fim de promover maior clareza e precisão a seus enunciados, e no inciso VII do art. 2º, mediante o emprego de paralelismo, a fim de promover relação de simetria no texto. As redações suprimidas se encontram tachadas e as inseridas em negrito. Veja-se:

> CAPÍTULO I
>
> DAS DISPOSIÇÕES PRELIMINARES
>
> Art. 1º ~~Este Regulamento tem por objetivo normatizar o processo de~~ **A** comunicação de incidente de segurança com dados pessoais que possa acarretar risco ou dano relevante aos titulares **obedecerá ao disposto neste Regulamento**, nos termos do art. 48 da Lei nº 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD).
>
> Art. 2º O ~~processo de comunicação de incidente de segurança com dados pessoais atenderá aos seguintes objetivos~~ **São objetivos deste Regulamento**:
>
> I - proteger os direitos dos titulares;
>
> II - assegurar a adoção das medidas necessárias para mitigar ou reverter os efeitos dos prejuízos gerados;
>
> III - ~~incentivar~~ **assegurar a efetividade d**o princípio da responsabilização e da prestação de contas pelos agentes de tratamento;
>
> IV - promover a adoção de regras de boas práticas e de governança e de medidas de prevenção e segurança adequadas;

V - estimular a promoção da cultura de proteção de dados pessoais;

VI - garantir que os agentes de tratamento atuem de forma transparente, e estabeleçam uma relação de confiança com o titular; e

VII - fornecer subsídios para as atividades **regulatória**~~s~~, ~~de fiscalização~~ **fiscalizatória** e ~~sancionadora~~ **sancionatória** da Autoridade Nacional de Proteção de Dados (ANPD).

Regulamento - Cap. II - Das Definições:

63. A minuta do regulamento colocada em consulta pública tem o seguinte texto para esta seção:

CAPÍTULO II

DAS DEFINIÇÕES

ART. 3º Para efeitos deste Regulamento, são adotadas as seguintes definições:

I - ampla divulgação do incidente em meios de comunicação: providência que pode ser determinada pela ANPD ao controlador, nos termos do art. 48, § 2º, I, da LGPD, no âmbito do processo de comunicação de incidente de segurança com dados pessoais, como a publicação no sítio da Internet e nas redes sociais do controlador ou em outros meios de grande alcance;

II - autenticidade: propriedade pela qual se assegura que o dado pessoal foi produzido, expedido, modificado ou destruído por uma determinada pessoa física, equipamento, sistema, órgão ou entidade;

III - categoria de dados pessoais: classificação dos dados pessoais de acordo com o contexto de sua utilização, como identificação pessoal, autenticação em sistemas, financeiro, saúde, educação e judicial;

IV - comunicação do incidente de segurança: ato do controlador que comunica à ANPD e ao titular de dados a ocorrência de incidente de segurança com dados pessoais que possa acarretar risco ou dano relevante aos titulares;

V - confidencialidade: propriedade pela qual se assegura que o dado pessoal não esteja disponível ou não seja revelado a pessoas, sistemas, órgãos ou entidades não autorizadas e nem credenciadas;

VI - dado de autenticação em sistemas: qualquer dado pessoal utilizado como credencial para determinar o acesso a um sistema ou para confirmar a identificação de um usuário, como contas de login, *tokens* e senhas;

VII - dado financeiro: dado pessoal relacionado às transações financeiras do titular, inclusive para contratação de serviços e aquisição de produtos;

VIII - dado pessoal afetado: dado pessoal cuja confidencialidade, integridade, disponibilidade ou autenticidade tenha sido comprometida em um incidente de segurança;

IX - disponibilidade: propriedade pela qual se assegura que o dado pessoal esteja acessível e utilizável, sob demanda, por uma pessoa física ou determinado sistema, órgão ou entidade devidamente autorizados;

X - incidente de segurança com dados pessoais: qualquer evento adverso confirmado, relacionado à violação das propriedades de confidencialidade, integridade, disponibilidade e autenticidade da segurança de dados pessoais;

XI - integridade: propriedade pela qual se assegura que o dado pessoal não seja modificado ou destruído de maneira não autorizada ou acidental;

XII - medidas de segurança relacionadas a dados pessoais: medidas técnicas e administrativas adotadas para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração ou comunicação;

XIII - natureza dos dados pessoais: classificação de dados pessoais em gerais ou sensíveis;

XIV - procedimento de apuração de incidente de segurança: procedimento realizado pela ANPD para apurar a ocorrência de incidente de segurança com dados pessoais capaz de acarretar risco ou dano relevante ao titular que não tenha sido comunicado pelo controlador;

XV - procedimento de comunicação de incidente de segurança: procedimento no âmbito da ANPD que abrange a comunicação do incidente com dados pessoais capaz de acarretar risco ou dano relevante ao titular e a avaliação da necessidade de determinação de adoção de providências;

XVI - processo de comunicação de incidente de segurança com dados pessoais: processo instaurado no âmbito da ANPD, com o objetivo de verificar a ocorrência de incidentes de segurança com dados pessoais capazes de acarretar risco ou dano relevante aos titulares de dados, podendo abranger o procedimento de apuração de incidente de segurança e o procedimento de comunicação de incidente de segurança; e

XVII - relatório de tratamento de incidente: relatório fornecido pelo controlador que contém cópias, em meio físico ou digital, de documentos, dados e informações relevantes para descrever o incidente e as ações adotadas para o seu tratamento, tais como, evidências e cronologia do incidente, metodologia de investigação e ferramentas utilizadas, e medidas de segurança adotadas.

Contribuições recebidas:

64. Das 223 (duzentas e vinte e três) contribuições apresentadas para este capítulo, destacam-se, pela relevância, as sugestões descritas abaixo.

65. Sugeriu-se alteração, ao longo do texto do regulamento, dos

termos incidentes de segurança para incidentes de segurança com dados pessoais, de forma que reflita a conceituação estabelecida no art. 3º. Recomendou-se a criação de um glossário pela ANPD, de forma a uniformizar as conceituações entre normativos expedidos pela Autoridade. Houve, também, dúvidas e sugestões de definição mais clara do que seria considerado eficaz para atingir ampla divulgação na comunicação dos incidentes de segurança com dados pessoais. Várias contribuições sustentam preocupação com relação à comunicação do incidente de segurança com dados pessoais não se confundir com a sanção administrativa de publicização da infração prevista no art. 20 da Resolução CD/ANPD nº 4.

66. Houve sugestões para que seja excluído ou revisto o inciso III, do art. 3º, o qual trata da conceituação de categoria de dado pessoal, uma vez que as categorias listadas no regulamento não constam na LGPD. Ainda, sugestões quanto à adequação do termo "confidencialidade", presente no art. 3º, V, no sentido de eliminar partes da definição ou discutir a questão da autorização presente na conceituação. Igualmente, houve contribuições com fins de eliminar o rol exemplificativo "como contas de login, tokens e senhas" do inciso VI do art. 3º, tendo como base que não seriam considerados dados pessoais à luz da LGPD.

67. Sugeriu-se a exclusão ou alteração quanto à incorporação do conceito de autenticidade (art. 3º, II) e à definição de "dado pessoal afetado" (art. 3º, VIII), a qual cita o termo autenticidade. Também houve sugestões acerca da complementação, alteração e exclusão do conceito de "dado financeiro", inciso VII do art. 3º do regulamento. Ainda, houve contribuições destinadas a alterar o conceito de incidente de segurança com dados pessoais para que se assemelhe ao art. 46 da LGPD ou ao GDPR. Recomendou-se alterar a redação do inciso XIII do art. 3º do RCIS, a fim de se excluir o termo "em gerais", em conformidade com o que dispõe a LGPD.

68. Houve, ainda, sugestões de inclusão, no art. 3º, XV, de indicação de que é o controlador quem deve realizar a comunicação objeto do procedimento de comunicação de incidente de segurança. Por fim, sugeriu-se alterar a nomenclatura processo de comunicação de incidente de segurança com dados pessoais (art. 3º, XVI) para processo de averiguação de segurança com dados pessoais, de forma a evitar confusão, devido à denominação similar, com o procedimento de comunicação de incidente de segurança (art. 3º, XV).

Análise:

69. Em atenção às várias sugestões que solicitaram a complementação do termo "incidente de segurança" por "incidente de segurança com dados pessoais", de forma a seguir a definição constante no art. 3º, inciso X, julgou-se parcialmente pertinente a alegação, com a realização da padronização do texto de identificação de Capítulos e de Seções da minuta.

70. Quanto à sugestão de ANPD publicar um glossário, concorda-se com a proposição, inclusive lança-se luz à importância de tal publicação, frente aos vários normativos que foram e serão publicados pela Autoridade. Entretanto, a sugestão não tem relação com o escopo do Regulamento ora em análise.

71. Em atenção à ampla divulgação do incidente em meios de comunicação, a grande preocupação foi referente à necessidade de diferenciá-la da sanção administrativa de publicização constante no art. 20 da Resolução CD/ANPD nº 4. No entanto, a divulgação mencionada no art. 48, § 2º, inciso I, relacionada à comunicação de incidentes, não se confunde com a publicização expressa no art. 52, inciso IV, referente às sanções administrativas, ambos artigos da LGPD. A ampla divulgação ocorre no âmbito do comunicação de incidente, quando a ANPD entende que a comunicação realizada não alcançou o objetivo esperado, já a sanção de publicização da infração ocorre após devidamente apurada e confirmada a sua ocorrência, nos termos dos arts. 20 e 21 do Regulamento de Dosimetria. No entanto, para trazer entendimento mais direto a minuta proposta, incluiu-se o §7º no art. 19, que dispõe que os dispositivos regulamentares não se confundem.

72. Quanto à exclusão do inciso III do art. 3º, a equipe de projeto opinou no sentido de que a ANPD, enquanto entidade reguladora e fiscalizadora, detém o poder de regulamentar o modo como os agentes regulados deverão dispor das informações deles requeridas, o que inclui a definição de categorias de dados pessoais não previstas na LGPD.

73. Quanto à conceituação de confidencialidade, objeto de várias contribuições, de forma geral, julgou-se procedente a supressão do termo “nem credenciadas”, uma vez que se entende que pessoas, sistemas, órgãos ou entidades credenciadas e não autorizadas não devam ter acesso aos dados, ou seja, há uma incongruência gerada com a permanência do termo. Ademais, o conceito de confidencialidade, baseado em normativos como a ISO/IEC 27002:2022 e outros, tem como premissa a autorização da disponibilidade e da divulgação da informação, motivo pelo qual entende-se pela impossibilidade de supressão do termo autorizadas.

74. Em atenção ao rol exemplificativo constante no inciso VI do art. 3º, o qual algumas sugestões alegam que não pode ser considerado como dados pessoais à luz da LGPD, esclarece-se que, por estar no contexto de associação a um login ou identificador único de um indivíduo, esses podem ser considerados como dados pessoais, em contraposição ao sustentado nas contribuições.

75. Referente às sugestões de exclusão, alteração e adaptação de excertos constantes no texto do Regulamento que referenciam o termo autenticidade, julgou-se procedente a exclusão da sua conceituação e de todas as referências ao longo do texto, uma vez que, a despeito de haver correntes doutrinárias que colocam a autenticidade como um dos pilares da

segurança da informação, a equipe de projeto entendeu que não cabe à ANPD empreender ações de fiscalização quanto à autenticidade, indo ao encontro do exposto na Nota Técnica nº 12/2023/CGN/ANPD (4012432), do parágrafo 239 ao 254.

76. Em relação às sugestões acerca da alteração ou exclusão do termo dado financeiro, cabe mencionar que as experiências internacionais subsidiam a inclusão dessa categoria na definição de incidente de segurança com risco ou dano relevante, tendo em vista a evidente relação entre essa categoria de dado pessoal e o risco de perdas financeiras que um incidente de segurança envolvendo esse tipo de dado pode trazer ao titular. A definição proposta de dados financeiros foi inspirada na regulação dos Estados Unidos de proteção das informações financeiras do consumidor (Privacy of Consumer Financial Information Regulation).

77. No tocante à definição de incidente de segurança com dados pessoais assemelhada ao disposto no art. 46 da LGPD ou ao GDPR, a Nota Técnica nº 12/2023/CGN/ANPD externou, especialmente em seus parágrafos 62, 63 e 65, que o art. 46 da LGPD "não abarca indiretamente a definição do termo incidente de segurança [...] convém pontuar que o termo técnico incidente de segurança não foi criado pela LGPD, e já existia na área de segurança da informação a fim de definir situações que podem ocorrer no âmbito de operações com informações". Portanto, tais contribuições não foram incorporadas à proposta de regulamentação.

78. Quanto às sugestões com a justificativa de harmonizar a redação da minuta de Regulamento com a LGPD, a fim de excluir o termo “em gerais” do inciso XIII do art. 3º, os participantes entendem que a LGPD categoriza os dados em dois tipos de dados: “dado pessoal” e “dado pessoal sensível”. No entanto, não se trata de uma categorização estrita, pois todo dado pessoal sensível é dado pessoal, mas nem todo dado pessoal é dado pessoal sensível. Entende-se que dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural, é parte do todo informação relacionada a pessoa natural identificada ou identificável. Em outros termos, dado pessoal sensível é uma espécie do gênero dado pessoal. O termo sensível, assim, direciona tratamento legal distinto, específico, aos dados pessoais que não são tidos como sensíveis. A ideia de se incluir, no regulamento, o termo geral, embora não previsto na LGPD, tem a finalidade de se fazer referência clara e precisa àqueles dados pessoais que não são qualificados como sensíveis pela lei. Não se pode negar que a LGPD estabeleceu duas naturezas para os dados pessoais: sensível e, por exclusão, não sensível. A CGN escolheu, desde o início do processo de regulamentação, referir-se aos dados pessoais não sensíveis como dados pessoais gerais.

79. Em atenção às sugestões de inserção do controlador como o responsável pela comunicação objeto do procedimento de comunicação de

incidentes de segurança, julga-se pertinente, tendo em vista o disposto no art. 48 da LGPD; e

80. Com relação à nomenclatura similar entre "processo de comunicação de incidente de segurança com dados pessoais" (art. 3º, XVI) e "procedimento de comunicação de incidente de segurança" (art. 3º, XV), entende-se que pode haver certa "confusão" em um primeiro momento, entretanto, com a leitura do regulamento, é possível depreender a conceituação distinta de cada um dos dispositivos.

Proposta de nova redação para os dispositivos em pauta:

81. Após a análise das contribuições acima citadas, apresenta-se, a seguir, nova proposta de redação, incluindo-se ajustes de ofício, pela equipe de projeto, no inciso XVI, e inclusão de definição sobre dado protegido por sigilo legal ou judicial, no inciso VIII, em virtude de contribuição relacionada ao art. 5º do Regulamento, além da inclusão da definição sobre dado protegido por sigilo profissional, no inciso IX. As redações suprimidas se encontram tachadas e as inseridas em negrito:

> CAPÍTULO II
>
> DAS DEFINIÇÕES
>
> ART. 3º Para efeitos deste Regulamento, são adotadas as seguintes definições:
>
> I - ampla divulgação do incidente em meios de comunicação: providência que pode ser determinada pela ANPD ao controlador, nos termos do art. 48, § 2º, I, da LGPD, no âmbito do processo de comunicação de incidente de segurança com dados pessoais, como a publicação no sítio **eletrônico** ~~da Internet~~ e nas redes sociais do controlador ou em outros meios de grande alcance;
>
> ~~II - autenticidade: propriedade pela qual se assegura que o dado pessoal foi produzido, expedido, modificado ou destruído por uma determinada pessoa física, equipamento, sistema, órgão ou entidade;~~
>
> ~~III~~ **II** - categoria de dados pessoais: classificação dos dados pessoais de acordo com o contexto de sua utilização, como identificação pessoal, autenticação em sistemas, financeiro, saúde, educação e judicial;
>
> ~~IV~~ **III** - comunicação do incidente de segurança: ato do controlador que comunica à ANPD e ao titular de dados a ocorrência de incidente de segurança com dados pessoais que possa acarretar risco ou dano relevante aos titulares;
>
> ~~V~~ **IV** - confidencialidade: propriedade pela qual se assegura que o dado pessoal não esteja disponível ou não seja revelado a pessoas, sistemas, órgãos ou entidades não autorizadas ~~e nem credenciadas~~;
>
> ~~VI~~ **V** - dado de autenticação em sistemas: qualquer dado pessoal utilizado como credencial para determinar o acesso a um sistema ou para confirmar a identificação de um usuário, como contas de login,

tokens e senhas;

~~VII~~ **VI** - dado financeiro: dado pessoal relacionado às transações financeiras do titular, inclusive para contratação de serviços e aquisição de produtos;

~~VIII~~ **VII** - dado pessoal afetado: dado pessoal cuja confidencialidade, integridade~~,~~ **ou** disponibilidade ~~ou autenticidade~~ tenha sido comprometida em um incidente de segurança;

VIII - dado protegido por sigilo legal ou judicial: dado pessoal cuja proteção decorra de lei ou decisão judicial;

IX - dado protegido por sigilo profissional: dado pessoal cuja proteção decorra do exercício de função, ministério, ofício ou profissão, e cuja revelação possa produzir dano a outrem;

~~IX~~ X - disponibilidade: propriedade pela qual se assegura que o dado pessoal esteja acessível e utilizável, sob demanda, por uma pessoa física ou determinado sistema, órgão ou entidade devidamente autorizados;

~~X~~ XI - incidente de segurança com dados pessoais: qualquer evento adverso confirmado, relacionado à violação das propriedades de confidencialidade, integridade~~,~~ **e** disponibilidade ~~e autenticidade~~ da segurança de dados pessoais;

~~XI~~ XII- integridade: propriedade pela qual se assegura que o dado pessoal não seja modificado ou destruído de maneira não autorizada ou acidental;

~~XII~~ XIII - medidas de segurança relacionadas a dados pessoais: medidas técnicas e administrativas adotadas para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração ou comunicação;

~~XIII~~ XIV - natureza dos dados pessoais: classificação de dados pessoais em gerais ou sensíveis;

~~XIV~~ XV - procedimento de apuração de incidente de segurança: procedimento realizado pela ANPD para apurar a ocorrência de incidente de segurança com dados pessoais **que não tenha sido comunicado pelo controlador capaz** de acarretar risco ou dano relevante ao titular ~~que não tenha sido comunicado pelo controlador~~;

~~XV~~ XVI - procedimento de comunicação de incidente de segurança: procedimento no âmbito da ANPD que abrange a comunicação do incidente com dados pessoais**, a ser realizada pelo controlador,** capaz de acarretar risco ou dano relevante ao titular e a avaliação da necessidade de determinação de adoção de providências;

~~XVI~~ XVII - processo de comunicação de incidente de segurança com dados pessoais: processo **administrativo** instaurado no âmbito da ANPD, com o objetivo de verificar a ocorrência de incidentes de segurança com dados pessoais capazes de acarretar risco ou dano relevante aos titulares de dados, podendo abranger o procedimento de apuração de incidente de segurança e o procedimento de comunicação de incidente de segurança; e

~~XVII~~ XVIII - relatório de tratamento de incidente: relatório fornecido

pelo controlador que contém cópias, em meio físico ou digital, de documentos, dados e informações relevantes para descrever o incidente e as ações adotadas para o seu tratamento, tais como, evidências e cronologia do incidente, metodologia de investigação e ferramentas utilizadas, e medidas de segurança adotadas.

Regulamento - Cap. III - Seção I - Dos critérios para comunicação do incidente de segurança:

82. A minuta do regulamento colocada em consulta pública tem o seguinte texto para essa seção:

> CAPÍTULO III
>
> DA COMUNICAÇÃO DE INCIDENTE DE SEGURANÇA
>
> Art. 4º O controlador deverá comunicar à ANPD e ao titular os incidentes de segurança com dados pessoais que possam acarretar risco ou dano relevante aos titulares.
>
> Art. 5º Para fins deste Regulamento, considera-se que um incidente de segurança com dados pessoais pode acarretar risco ou dano relevante aos titulares quando tiver potencial de afetar significativamente interesses e direitos fundamentais dos titulares e envolver pelo menos um dos seguintes critérios:
>
> I - dados sensíveis;
>
> II - dados de crianças, de adolescentes ou de idosos;
>
> III - dados financeiros;
>
> IV - dados de autenticação em sistemas;
>
> V - dados em larga escala.
>
> § 1º São considerados incidentes que têm potencial de afetar significativamente interesses e direitos fundamentais dos titulares aqueles que possam:
>
> I - impedir ou limitar o exercício de direitos ou a utilização de um serviço; ou
>
> II - ocasionar danos materiais ou morais aos titulares, tais como discriminação, violação à integridade física, ao direito à imagem e à reputação, fraudes financeiras ou uso indevido de identidade.
>
> § 2º Para aplicação deste Regulamento, os incidentes de segurança com dados pessoais em larga escala serão assim caracterizados quando abrangerem número significativo de titulares, considerando, ainda, o volume de dados envolvidos e a extensão geográfica de localização dos titulares.
>
> § 3º A ANPD poderá publicar orientações com o objetivo de auxiliar os agentes de tratamento na avaliação do incidente que possa acarretar risco ou dano relevante ao titular.

Contribuições recebidas:

83. Das contribuições apresentadas para este capítulo, destacam-

se, pela relevância, as sugestões descritas abaixo:

84. Quanto ao art. 4º da minuta do Regulamento, houve 13 (treze) contribuições. As sugestões foram no sentido de incluir hipóteses explícitas de casos em que não é necessário comunicar um incidente de segurança à ANPD e/ou aos titulares, em razão das diferentes finalidades do ato de comunicação aos dois destinatários, ou de que haja comunicação ao titular apenas quando houver alto risco; de limitar os casos de comunicação à ANPD, a exemplo de Regulamentações da HIPAA, que indicam a necessidade de comunicação em caso de violações envolvendo 500 ou mais indivíduos; de qualificar o termo incidentes de segurança com dados pessoais com o modificador confirmados, em virtude da definição presente no inciso X do art. 3º da minuta da Regulamento.

85. Já para o art. 5º, foram 236 (duzentas e trinta e seis) contribuições no total. Destacam-se, pelo volume e relevância, as sugestões adiante.

86. Em relação à redação do caput do artigo 5º, 16 (dezesseis) contribuições manifestaram preocupação quanto a sua interpretação, pois a redação não deixa clara a necessidade de conjugar o disposto no caput com pelo menos um dos incisos, na tomada de decisão para efetuar a comunicação do incidente. Em efeito, pode-se interpretar o conectivo “e” como “ou”, no caput.

87. Houve 3 (três) sugestões de inclusão da expressão “quando ocorridos em larga escala” no caput do artigo, pois, dessa maneira, resultaria apenas a comunicação de incidentes que atendessem necessariamente essa condição, concomitantemente com um dos incisos propostos.

88. 7 (sete) contribuições observaram a necessidade de adequar a redação à terminologia da LGPD, adicionando a palavra “pessoais” no inciso I do art. 5º para “dados pessoais sensíveis”.

89. Em referência ao termo “idoso”, do inciso II do art. 5º, 29 (vinte e nove) contribuições foram no sentido de excluí-lo. Argumentou-se que a Regulamentação deve observar a LGPD, sem extrapolar os limites legais estabelecidos pela norma. Do que se observa da LGPD, são estabelecidas apenas duas categorias de dados, dados pessoais e dados sensíveis. Desta forma, propõe-se a supressão dos demais tipos de dados ou sujeitos que não estejam expressamente definidos na LGPD, de modo a garantir uma regulação com segurança jurídica e em conformidade com o processo de produção normativa infralegal.

90. Houve 2 (duas) contribuições para incluir outras categorias relacionadas a vulneráveis no Inciso II do art .5º. Sugeriram a ampliação das categorias relacionadas vulneráveis, para abarcar, além de crianças, adolescentes e idosos, categorias como incapazes e portadores de necessidades especiais.

91. Por meio de 4 (quatro) contribuições, sugeriu-se a supressão do

inciso III do art. 5º, qual seja, dados financeiros, com a justificativa de que haveria um volume considerável de incidentes que teriam de ser notificados, sobrecarregando a ANPD de forma desnecessária. Adicionalmente, que essa categoria não está citada na LGPD, ao contrário de outros incisos, e que não compete estabelecer categorias especiais de dados quando o legislador assim não o fez.

92. 11 (onze) contribuições, a fim de excluir o critério “dados de autenticação em sistemas', no inciso IV do art. 5º, trouxeram argumentos no sentido de que deve haver preocupação, por parte da ANPD, sobre as informações a que os dados de autenticação dão acesso e sobre os dados de autenticação em si. Além disso, argumenta-se que o dado pessoal utilizado como credencial para determinar a identificação de um usuário, como contas de login, já faz parte de outras categorias de dados, como dados de identificação (e-mail, CPF e telefone).

93. 3 (três) contribuições sugeriram a supressão da expressão “tiver potencial” do Inciso I do parágrafo 1º, pois a referida expressão, conjugada com “afetar significativamente interesses e direitos dos titulares”, implica em ampla margem para o que pode ser considerado incidente de segurança a ser comunicado para a ANPD. Desta forma, a atual definição, se aprovada, abrangeria uma infinidade de casos e proporcionaria um esvaziamento da própria funcionalidade do instituto da notificação.

94. Mediante 3 (três) contribuições, sugeriu-se a inserção de nova categoria de dados pessoais, como critério de comunicação, qual seja, dados pessoais protegidos por sigilo legal ou profissional. A justificativa foi no sentido de que a ANPD menciona, na sua página de esclarecimentos sobre comunicação de incidentes, dados pessoais protegidos por sigilo profissional como exemplo de hipótese em que é necessário notificar a Autoridade. Dessa forma, entendeu-se ser pertinente ter essa previsão no Regulamento, a fim de que informações como, por exemplo, listas de proteção à testemunha também sejam abarcadas.

95. 2 (duas) contribuições solicitaram a inclusão do termo “comprovadamente” no § 1º do art. 5º, de modo que o texto seja: “são considerados incidentes que têm potencial de afetar significativamente interesses e direitos fundamentais dos titulares aqueles que comprovadamente possam (...)”. Embora não tenha havido justificativa apresentada por parte dos participantes, infere-se que a intenção foi suprimir o fator probabilidade na mensuração do risco, de forma que apenas os incidentes com danos concretos aos titulares sejam comunicados.

96. Quanto ao inciso II do § 1º art. 5º, houve 8 (oito) contribuições a fim de suprimir a expressão “danos morais ou materiais aos titulares”. Argumenta-se no sentido de que a comprovação do nexo de causalidade sobre o que efetivamente poderia ocasionar dano moral ou material deveria ser verificada na esfera judicial e não administrativa, como se propõe, e que não há que se levar em consideração requisitos sobre danos morais e materiais como precedentes a uma comunicação de um incidente.

97. 21 (vinte e uma) contribuições foram no sentido de suprimir o inciso I do § 1º. Argumentou-se, resumidamente, que o termo "limitação de exercício de direitos" pode gerar ampla interpretação e ocasionar situações em que a limitação será razoável ao caso concreto, como, por exemplo, a limitação de acessos em sistema afetado por um incidente, a fim de mitigar danos aos titulares afetados e que, per se, não deveria ser caracterizado como ilícito. Já o termo "serviço" extrapolaria a aplicação da LGPD que se atém a regular o tratamento de dados pessoais.

98. Houve 10 (dez) contribuições no sentido de alterar da redação do parágrafo 3º do art. 5º, substituindo "poderá publicar" para "publicará", pois manifestaram preocupação na interpretação do Regulamento e solicitaram a publicação de um guia orientativo ela ANPD.

99. Quanto à definição do conceito "larga escala" (inciso V do art. 5º), "número significativo de titulares" (§ 2º do art. 5º) e "extensão geográfica" (§ 2º do art. 5º), houve 68 (sessenta e oito) contribuições referentes a esse tema, no sentido de que não há, até o momento, dispositivo normativo que determine o que seria considerado "número significativo de titulares", o que inviabilizaria a aplicabilidade do Regulamento.

100. Recomendou-se, ainda, a utilização do critério de alto risco adotado no RIPD. 3 (três) contribuições sugeriram a adoção do critério de alto risco baseado nas definições estabelecidas no Relatório de Impacto de Proteção de Dados, uma vez que o atual Regulamento não esclarece quais seriam esses critérios, e também no sentido de padronizar normas.

101. Por fim, como recomendação geral, 2 (dois) participantes sugeriram a criptografia, a anonimização e as demais formas de indisponibilidade de dados como um fator que dispensaria a comunicação do incidente.

Análise:

102. Em relação às contribuições para o art. 4º da minuta do Regulamento, a fim de explicitar hipóteses em que não seria necessário comunicar um incidente de segurança à ANPD e/ou aos titulares, deve-se recordar o disposto no art. 48 da LGPD, dispositivo respeitante à comunicação de ocorrência de incidente de segurança com dados pessoais, a seguir:

> 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.

103. De sua leitura, destaca-se do caput do artigo a atribuição, ao controlador, do dever de comunicar a ocorrência de incidente que possa acarretar risco ou dano relevante aos titulares, tanto à ANPD quanto aos titulares. Além disso, observa-se que não há distinção entre graus de relevância do risco (baixo, moderado ou alto, conforme se gradua em termos de gerenciamento de riscos) ou do dano (extensão do dano, conforme linguagem do art. 944 do Código Civil), de modo a se fazer diferenciação quanto a hipóteses em que o controlador deveria comunicar somente à ANPD, por exemplo.

104. Isso posto, o termo “relevante” não parece ser necessariamente sinônimo do termo “alto”, no sentido de se entender que o legislador indicou que deve haver comunicação à autoridade e ao titular em caso de incidente capaz de acarretar risco alto ou dano de grande extensão. No entanto, como se trata de um termo vago, cabe à ANPD definir se o risco ou dano relevante ao titular que gerará o dever de comunicar é apenas aquele qualificado como alto ou de grande extensão, respectivamente. Em outros termos, compete à autoridade nacional definir o que deve ser considerado como significativo ou importante, de modo a gerar comunicação tanto ao titular quando à ANPD.

105. Cumpre elucidar, igualmente, se, no exercício de seu poder normativo, pode a ANPD distinguir entre as situações em que ela deveria ser comunicada e as situações em que os titulares afetados deveriam ser comunicados. Em outras palavras, se é possível definir requisitos diferentes para a comunicação ao titular e para a comunicação à ANPD.

106. Certos participantes opinaram que é possível haver critérios ou requisitos distintos, pois a diferenciação quanto aos elementos da

comunicação a um e a outro, nos termos da atual redação dos arts. 6º e 9º da minuta do Regulamento e os objetivos diferentes de cada comunicação apontariam nesse sentido.

107. Desse modo, recomendam que a comunicação à autoridade deve ocorrer sempre que houver risco ou dano relevante, enquanto a comunicação aos titulares deve ocorrer somente quando a gravidade desse risco ou dano for considerada mais alta em relação aqueles que precisam ser notificados à ANPD. Infere-se que o recomendado seria que, envolvendo situações de risco ou dano relevante aos titulares (gravidade baixa, média ou alta), o incidente deveria ser comunicado à autoridade nacional. Somente quando o incidente envolvesse risco ou dano de maior gravidade aos titulares é que estes deveriam ser comunicados.

108. A CGN tem o entendimento de que o art. 48 da LGPD não abarca essa possibilidade e que esta seria uma diferença entre a LGPD e o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, o Regulamento Geral de Proteção de Dados (RGPD).[4]

109. O ato legislativo europeu define que uma violação de dados deve ser comunicada à autoridade de controle quando resultar em um risco aos direitos e liberdades do titular e ao titular quando implicar elevado risco a essas liberdades e direitos. A lei brasileira estabelece que o controlador deverá comunicar à autoridade nacional e aos titulares a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

110. Observa-se que o legislador pátrio foi claro em sua vontade de não estabelecer diferenciação quanto a gradação de riscos ou danos ao titular, tal como o faz o legislador europeu.

111. Caso a ANPD regulamentasse que risco ou dano relevante aos titulares, para fins de comunicação ao titular, fosse situações de alta gravidade, e, para fins de comunicação à autoridade nacional, fosse situações de baixa, média ou alta gravidade, estar-se-ia deixando de cumprir o mandamento legal em sua totalidade. Portanto, a CGN considera que o critério ou gatilho disparador da comunicação de incidente de segurança com dados pessoais é único para o titular e para a autoridade nacional, sendo esta uma diferença entre LGPD e RGPD, conforme registrado acima.

112. No entanto, a CGN entende que a LGPD permite interpretação de que o prazo razoável para cada uma das comunicações pode ser estabelecido com valor igual ou diferente e, ainda, com início de contagem em momento igual ou diferente, uma vez que os objetivos e propósitos de cada comunicação são distintos. Enquanto para a ANPD é no sentido de garantir um direito fundamental, zelar pela proteção de dados e ter a possibilidade de investigar práticas gerais de controladores, para o titular de dados é no sentido de ser informado ou conscientizado sobre os riscos que enfrenta, a fim de que tome medidas necessárias para resguardar seus direitos, de modo a promover o princípio da transparência. Além disso, a

CGN afiliou-se ao entendimento de que os incisos do § 1º do art. 48, referentes ao conteúdo da comunicação, são comuns aos dois destinatários, ANPD e titular de dados, pois o § 1º da LGPD não abre possibilidade para se deixar de comunicar determinadas informações ao titular. Ao contrário, estabelece informações mínimas para a comunicação, deixando em aberto o acréscimo de informações. Por essa razão, na seção desta Nota Técnica referente ao art. 9º, que trata da comunicação ao titular de dados, constarão as inclusões referentes aos incisos que não haviam sido considerados na minuta do Regulamento pré-consulta pública. No entanto, a CGN manifesta reservas quanto à menção do conteúdo disposto no inciso II do § 1º do art. 48, informações sobre os titulares envolvidos, na comunicação individualizada aos titulares, por entender que esse inciso se refere sobre a identificação dos titulares e não caberia informar a um titular informações sobre os demais, mas somente à ANPD. Por essa razão, surge uma dúvida jurídica a ser dirimida pela PFE/ANPD quanto à possibilidade de não inclusão desse conteúdo na comunicação ao titular, em que pese conste da LGPD como elemento mínimo a ser mencionado nessa comunicação.

113. No que tange à proposta de adoção do critério de alto risco para fins de comunicação de incidente de segurança, baseado na mesma diretiva do relatório 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 na LGPD, recorda-se que o art. 48 da LGPD não restringe a comunicação de incidente aos casos de alto risco. Adicionalmente, conforme o parágrafo 272 da Nota Técnica 12 (4012432), o conceito de tratamento de alto risco, que envolve contexto diferente de incidente com risco ou dano relevante, tendo em vista tratar-se de todo o tratamento e não somente do incidente de segurança, já está sendo tratado pela ANPD em processo específico.

114. Quanto ao caput do art. 5º, no que concerne à interpretação do caput do artigo, houve, aparentemente, má compreensão do texto da norma. O que a contribuição sugere está de acordo com o parágrafo 91 da Nota Técnica 12 (4012432), que cita a conjugação do critério de potencial de afetar significativamente interesses e direitos fundamentais com, pelo menos, um dos critérios dos incisos. No sentido de sanar a dúvida, sugere-se que a redação seja alterada para "e, cumulativamente", de forma a evitar que esse "e" seja lido como um "ou".

115. No que se refere à inclusão de “quando ocorridos em larga escala” no caput do art. 5º, concluiu-se que condicionar a comunicação a esse critério resultaria na não comunicação de incidentes importantes, relacionados a dados sensíveis, por exemplo. Convém lembrar que incidente de segurança com dados pessoais ou vazamentos de dados que possam acarretar risco o dano relevante ao titular não se relaciona necessariamente com grande volume de dados. Assim, não se vê razão para essa alteração.

116. Em relação à supressão do termo “tiver potencial” do caput do art. 5º, importa esclarecer que o conceito de risco está atrelado à

probabilidade de um dano ocorrer. Essa redação parafraseia o texto do próprio caput do art. 48 da LGPD, pois trata da ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares, isto é, uma potencialidade. Ademais, a principal função da comunicação do incidente é de impedir ou reduzir as suas chances de causar danos ao titular. Logo, possui um caráter preventivo. Dessa forma, mantém-se a redação atual.

117. Quanto à inclusão do termo “pessoais” no texto do inciso I do art. 5º, para que reflita a terminologia “dados pessoais sensíveis”, entendeu-se que, embora não seja uma modificação significativa, é um ajuste que homenageia a precisão, pois é o mesmo termo trazido pela LGPD, onde, das nove ocorrências de "sensível/sensíveis", oito delas são como "dado(s) pessoal(is) sensível(is)". Portanto, a sugestão de alteração do texto é justa.

118. Em relação ao inciso II do art. 5º, referente às categorias de dados pessoais sensíveis, de crianças, de adolescentes e de idosos, importa lembrar que a alínea "d" do inciso II do art. 4º do Anexo I da Resolução CD/ANPD nº 2, de 27 de janeiro de 2002 (Regulamento de aplicação da LGPD para agentes de tratamento de pequeno porte) define dados de idosos como critério específico para qualificação do tratamento de alto risco. Em razão disso, por uma questão harmonização entre as normas editadas pela ANPD, busca-se manter atenção especial aos dados de idosos. Essa atenção decorre de que, embora a LGPD não tenha reservado tratamento especial a dados de idosos como o faz para os de crianças e adolescentes, a ANPD tem entendido que, pelo fato de idosos serem alvos fáceis de fraudes, a exemplo de golpes de empréstimo consignado, seus dados vazados podem dar margem a situações como essas. Com isso, a fim de mitigar esses riscos, a CGN entende que os dados de idosos devem permanecer na minuta do Regulamento.

119. Ademais, destaca-se que o art. 55-J, XIX, da LGPD, dispôs sobre a competência da ANPD de "garantir que o tratamento de dados de idosos seja efetuado de maneira simples, clara, acessível e adequada ao seu entendimento, nos termos desta Lei e da Lei nº 10.741, de 1º de outubro de 2003.”

120. Quando à sugestão de incluir dados de incapazes e de pessoas com deficiência, a CGN reconhece a vulnerabilidade dessas pessoas, mas não vislumbra, para o momento, incluir seus dados no rol de critérios para comunicação de incidentes de segurança com dados pessoais. Neste caso, entende-se mais adequado analisar o caso concreto. Para além disso, caso a ideia de sua inclusão esteja relacionada à sua condição de saúde ou médica, de acordo com o inciso II do artigo 5º da LGPD, esses dados são tidos como sensíveis, o que já está contemplado na minuta do Regulamento. Adicionalmente, a variedade de deficiências é muito alta, muitas delas não sendo incapacitantes ou limitantes do ponto de vista cognitivo. Com isso, o tratamento desse dado para uma finalidade que não esteja relacionada à deficiência pode sujeitar o titular a preconceito e riscos desnecessários.

121. Quanto à exclusão do inciso III, referente a “dados financeiros”, cabe mencionar que as experiências internacionais subsidiam a inclusão

dessa categoria na definição de incidente de segurança com risco ou dano relevante aos titulares, tendo em vista a evidente relação entre essa categoria de dado pessoal e o risco de perdas financeiras que um incidente de segurança envolvendo esse tipo de dado pode trazer ao titular. A definição proposta de dados financeiros foi inspirada na regulação estadunidense de proteção das informações financeiras do consumidor (Privacy of Consumer Financial Information Regulation1), que é parte do Gramm-Leach-Bliley Act. A regulação traz no § 1016.3, alínea "q", a definição de informações financeiras pessoalmente identificáveis (personally identifiable financial information), assim como exemplos do escopo de sua definição. Por essa razão, mantém-se o inciso.

122. Em relação à exclusão do inciso IV, referente a "autenticação em sistemas", a decisão de inclusão desse parâmetro baseia-se na literatura científica. O Direito Civil costuma relacionar riscos à privacidade com danos à honra, referidos como danos dignitários ou reputacionais. Além destes, existem problemas de privacidade mais modernos, de natureza socioestrutural, pois podem afetar a maneira como indivíduos se envolvem em certas atividades, podem privá-los de certas liberdades ou submetê-los a estruturas de poder que influenciam sua tomada de decisões e/ou geram efeitos inibitórios. A identificação é importante parâmetro para avaliar o risco ao titular de dados, pois a identificação conecta informações a titulares em particular. De maneira similar à agregação, combina diferentes peças de informação. Contudo, a identificação conecta essas informações a uma pessoa natural específica, como, por exemplo, a autenticação de usuários em sistema. Destarte, mantém-se o inciso IV.

123. Quanto à proposta de inserção de um novo inciso no caput do art. 5º, relacionado a "dados pessoais protegidos por sigilo legal ou profissional" como uma categoria relevante, a equipe de projeto entende pertinente, pois são informações protegidas por lei, considerando que sua violação pode resultar em riscos à integridade do titular.

124. No que tange à inserção do termo "comprovadamente" no texto do parágrafo 1º do art. 5º, a equipe de projeto considera não ser cabível, haja vista o cunho preventivo da comunicação do incidente, pois a LGPD e, consequentemente, o Regulamento em causa trata do risco de o incidente ocasionar um dano relevante ao titular, isto é, um conceito baseado em probabilidade.

125. Quanto à sugestão de se excluir o inciso I do § 1º do art. 5º, convém registrar que, dentre as hipóteses citadas na Nota Técnica 12 (SEI nº 4012432), inclui-se o caso em que o serviço prestado pelo agente de tratamento foi interrompido, mas não houve exposição dos titulares de dados pessoais e não afetou de forma expressiva os seus direitos. Nesse caso, a comunicação do incidente não seria necessária. Assim, compreende-se que o impedimento ou a limitação da utilização de um serviço deve ser analisado em conjunto com outros critérios, não sendo necessário suprimir ou mesmo restringir os serviços a que se refere o inciso em questão.

126. Em relação à supressão do texto “ocasionar danos morais ou materiais aos titulares” do inciso II do parágrafo 1º, o art. 48 da LGPD, ao estabelecer a obrigação de comunicação, faz referência à possibilidade de o incidente acarretar risco ou dano relevante aos titulares. Como bem mencionado na contribuição em questão, o STJ analisou a necessidade de comprovação para uma eventual indenização relativa a dano moral. A comunicação de ocorrência de incidente de segurança aos titulares busca informar ao titular da possibilidade de haver dano, não de que há ou de que haverá dano, além de medidas para mitigar esse risco. Dessa forma, não cabe ao agente de tratamento deliberar se houve efetivamente dano material ou moral ao titular em decorrência de um incidente de segurança, mas apenas se há risco de acarretar, ocasionar.

127. Referente ao § 2º do art. 5º, no que tange ao esclarecimento do termo “larga escala”, em razão das contribuições apresentadas, reconhece-se que ainda persiste a necessidade de maior esclarecimento sobre os termos "número significativo de titulares ou elevado volume de dados" e "extensão geográfica". No entanto, o projeto de guia sobre alto risco e larga escala já está e andamento no âmbito da Autoridade e tratará da questão.

128. No que concerne à alteração do parágrafo 3º do art. 5º, a fim de constar "publicará" em vez de "poderá publicar", no sentido de tornar obrigatória a publicação de orientações para auxiliar na interpretação da norma, convém lembrar que é de praxe da ANPD elaborar documentos auxiliares, como, por exemplo, guias, a fim de orientar os agentes regulados e os cidadãos em geral. Nessa esteira, considerando a conveniência e oportunidade administrativa, a ANPD poderá publicar orientações quanto à aplicação do regulamento em pauta, caso seja necessário. Desse modo, não se faz necessário alterar a redação do dispositivo.

129. Por fim, quanto à sugestão dos incidentes envolvendo dados pessoais criptografados ou tornados inacessíveis não serem relatados por não representar um risco significativo aos titulares dos dados, entende-se que, em razão do disposto nos §§ 2º e 3º do art. 48, o legislador não concedeu espaço para essa possibilidade. Nesses dispositivos, consta que a ANPD verificará a gravidade do incidente e avaliará eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis, no âmbito e nos limites técnicos dos serviços do controlador, para terceiros não autorizados a acessá-los. Desse modo, a comunicação de que trata o caput do art. 48 deve ser realizada mesmo quando os dados pessoais afetados estiverem criptografados ou tornados inacessíveis. Caso contrário, se o controlador deixar de comunicar à ANPD em virtude da ininteligibilidade dos dados pessoais afetados, a autoridade nacional nem fará juízo de gravidade do incidente nem avaliará comprovação da adoção das mencionadas medidas técnicas.

<u>Proposta de nova redação para os dispositivos em pauta:</u>

130. Após a análise das contribuições acima citadas, é apresentada a nova proposta redacional, sendo que as redações suprimidas se encontram tachadas e as inseridas em negrito, para melhor compreensão da proposta. Veja-se:

> CAPÍTULO III
>
> DA COMUNICAÇÃO DE INCIDENTE DE SEGURANÇA **COM DADOS PESSOAIS**
>
> Seção I
>
> Dos critérios para comunicação de incidente~~s~~ de segurança
>
> Art. 4º O controlador deverá comunicar à ANPD e ao titular **a ocorrência de** ~~os~~ incidente~~s~~ de segurança com dados pessoais que possa~~m~~ acarretar risco ou dano relevante aos titulares. Art. 5º Para fins deste Regulamento, considera-se que um incidente de segurança com dados pessoais pode acarretar risco ou dano relevante aos titulares quando tiver potencial de afetar significativamente interesses e direitos fundamentais dos titulares e**, cumulativamente**, envolver, pelo menos, um dos seguintes critérios:
>
> I - dados **pessoais** sensíveis;
>
> II - dados de crianças, de adolescentes ou de idosos;
>
> III - dados financeiros;
>
> IV - dados de autenticação em sistemas; ~~ou~~
>
> V - ~~**dados em larga escala**~~ **dados protegidos por sigilo legal, judicial ou profissional; ou**
>
> **VI - dados em larga escala**~~.~~
>
> § 1º ~~São considerados~~ **Considera-se** incidente~~s~~ que têm potencial de afetar significativamente interesses e direitos fundamentais dos titulares aquele~~s~~ que possa~~m~~:
>
> I - impedir ou limitar o exercício de direitos ou a utilização de um serviço; ou
>
> II - ocasionar danos materiais ou morais aos titulares, tais como discriminação, violação à integridade física, ao direito à imagem e à reputação, fraudes financeiras ou uso indevido de identidade.
>
> § 2º ~~Para aplicação deste Regulamento, os incidentes de segurança com dados pessoais em larga escala serão assim caracterizados quando abrangerem~~ **Considera-se incidente com dados em larga escala aquele que abranger** número significativo de titulares, considerando, ainda, o volume de dados envolvidos e a extensão geográfica de localização dos titulares.
>
> § 3º A ANPD poderá publicar orientações com o objetivo de auxiliar os agentes de tratamento na avaliação do incidente que possa acarretar risco ou dano relevante ao**s** titular**es**.

Regulamento - Cap. III - Seção II - Da comunicação do incidente à ANPD:

131. A minuta do regulamento colocada em consulta pública tem o seguinte texto para essa seção:

> Seção II
>
> Da comunicação do incidente de segura à ANPD
>
> Art. 6º A comunicação do incidente de segurança com dados pessoais à ANPD deverá ser realizada pelo controlador, no prazo de três dias úteis, ressalvada a existência de legislação específica, contados do conhecimento do incidente de segurança, sempre que o incidente possa acarretar risco ou dano relevante aos titulares afetados, e deve conter as seguintes informações:
>
> I - a descrição da natureza e da categoria de dados pessoais afetados;
>
> II - o número de titulares afetados, discriminando, quando aplicável, o número de crianças, de adolescentes ou de idosos;
>
> III - as medidas de segurança para a proteção dos dados pessoais adotadas antes e após o incidente;
>
> IV - os riscos relacionados ao incidente com identificação dos possíveis impactos aos titulares;
>
> V - os motivos da comunicação do incidente não ter sido realizada no prazo, se for o caso;
>
> VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do incidente sobre os titulares;
>
> VII - a data e a hora do conhecimento do incidente de segurança;
>
> VIII - os dados do encarregado, quando aplicável, ou do comunicante, acompanhado, nesta hipótese, de procuração ou outro instrumento com poderes para representar o controlador junto à ANPD;
>
> IX - os dados de identificação do controlador e, se cabível, declaração de tratar-se de agente de tratamento de pequeno porte;
>
> X - as informações sobre o operador, quando aplicável;
>
> XI - a declaração de que foi realizada a comunicação aos titulares, nos termos do art. 10 deste Regulamento;
>
> XII - a descrição do incidente, incluindo a causa principal, caso seja possível identificá-la; e
>
> XIII - o total de titulares cujos dados são tratados pela organização e na atividade de tratamento afetada pelo incidente.
>
> § 1º Excepcionalmente, as informações poderão ser complementadas, no prazo de vinte dias úteis, a contar do momento em que o controlador tomou conhecimento do incidente, prorrogável uma vez, por igual período, mediante solicitação fundamentada a ser avaliada pela ANPD.
>
> § 2º A comunicação do incidente de segurança deverá ocorrer por meio de formulário eletrônico, disponibilizado pela ANPD.
>
> § 3º A comunicação do incidente de segurança não será admitida quando apresentada por pessoa sem legitimidade.
>
> § 4º Caso o controlador seja representado por advogado, este poderá efetuar a comunicação sem procuração, obrigando-se a

apresentá-la no prazo de até quinze dias úteis, a contar da data da comunicação, sob pena desta não ser admitida.

§ 5º Nas hipóteses de não admissão da comunicação do incidente previstas nos §§ 3º e 4º, a ANPD poderá apurar a ocorrência do incidente de segurança por meio do procedimento de apuração de incidente de segurança, sem prejuízo da instauração de processo administrativo sancionador para avaliar o descumprimento do previsto nos arts. 6º e 9º deste Regulamento.

§ 6º O prazo constante no *caput* deste artigo conta-se em dobro para os agentes de pequeno porte, nos termos do disposto no Regulamento de aplicação da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) aos agentes de tratamento de pequeno porte, aprovado pela Resolução CD/ANPD nº 2, de 27 de janeiro de 2022.

Art. 7º Cabe ao controlador solicitar à ANPD, de maneira fundamentada, o sigilo de informações protegidas por lei, indicando aquelas cujo acesso deverá ser restringido, a exemplo das relativas à sua atividade empresarial cuja divulgação possa representar violação de segredo comercial ou industrial.

Art. 8º A ANPD poderá, a qualquer tempo, solicitar informações adicionais ao controlador, referentes ao incidente de segurança, inclusive o registro das operações de tratamento dos dados pessoais afetados pelo incidente, o relatório de impacto à proteção de dados pessoais (RIPD) e o relatório de tratamento do incidente, estabelecendo prazo para o envio das informações.

Contribuições recebidas:

132. Das contribuições apresentadas para esta seção, destacam-se, pelo volume e relevância, as seguintes sugestões:

133. Para o *caput* do art. 6º do anexo da minuta, grande parte das sugestões foram no sentido de alargar o prazo para comunicação do incidente à ANPD. Em vez de 3 (três) dias úteis, 5 (cinco), 7 (sete) ou 10 (dez) dias úteis. Ainda, 15 (quinze) ou 30 (trinta) dias também foram sugeridos. Os argumentos perpassam, por exemplo, pelo fato de que, no Brasil, há sobreposição regulatória e necessidade de comunicação não só à ANPD, mas também a outros órgãos regulatórios, devendo a comunicação ocorrer de forma coordenada. Cita-se, inclusive, que, no setor de seguros, a Circular Susep nº 638/2021 já determina o prazo de 5 (cinco) dias úteis, para fins de comunicação à Susep de incidente relevante.

134. A maioria dessas contribuições partiram do entendimento de que a mera data de conhecimento do incidente de segurança seria o termo inicial para a contagem desse prazo e de que o tempo seria bastante exíguo para avaliar se o incidente seria comunicável, isto é, para fazer a avaliação do incidente de segurança e do risco que dele pode resultar aos titulares dos dados pessoais afetados.

135. Dessa maneira, entende-se que muitas comunicações poderiam ocorrer desnecessariamente e a excepcionalidade do prazo de 20 (vinte) dias úteis para

complementação de informações tornar-se-ia a regra.

136. Houve sugestão no sentido de tornar claro que a comunicação se dará pelo controlador responsável pelo incidente, já que um tratamento de dados pessoais poderá ser realizado por dois controladores, nas hipóteses de co-controladoria, propondo-se a inclusão do termo "envolvido" após "controlador", resultando em "a comunicação deverá ser realizada pelo controlador envolvido (...)".

137. Houve, ainda, contribuição a fim de excluir a expressão “ressalvada a existência de legislação específica” e acrescentar a expressão “na forma descrita nesta Resolução”, pois não existiria ressalva sobre a legislação aplicável ao incidente de segurança.

138. Além disso, houve sugestão para mudar de "contados do *conhecimento* do incidente "para contados da *confirmação* do incidente", dentre outras. Também consta sugestão no sentido de incluir a expressão “pelo controlador”, de forma que passe a constar que o prazo de três dias úteis é contado do conhecimento, pelo controlador, do incidente de segurança, por suposta falta de clareza, dando margem ao entendimento de que poderia ser pelo operador.

139. Houve, ainda, afirmações no sentido de (i) haver incoerência em se ter o mesmo prazo para se comunicar à ANPD e aos titulares, (ii) se incluir parágrafo nesse artigo a fim de esclarecer que tomar conhecimento do incidente comunicável se dá com a avaliação sobre a possibilidade de acarretar risco ou dano relevante e (iii) haver um prazo, ainda que estendido, para avaliação da comunicabilidade do incidente de segurança envolvendo dados pessoais, pois, *passado esse período, todas as mazelas inerentes a vazamento de dados pessoais já estão feitas.*

140. Da leitura das contribuições sobre o caput do art. 6º, percebeu-se que houve entendimentos opostos sobre a intenção do dispositivo ou houve dúvidas sobre o que caracteriza tomar conhecimento do incidente, de modo a iniciar a contagem do prazo. Daí, observa-se que a redação minutada proporciona ambiguidade.

141. Nesse sentido, houve contribuição a fim de incluir parágrafo que explicitasse o que se considera como conhecimento do incidente, sugerindo que seja o momento a partir do qual o controlador tem razoável grau de certeza da ocorrência do incidente de segurança com dados pessoais, materializada com a ciência pelo Encarregado de Dados ou do responsável pelo canal de comunicação nos termos da Resolução CD/ANPD nº 2/2022, a seguir:

> §7º Em caso de impossibilidade de comunicar o incidente no prazo estipulado no caput, o agente de tratamento deverá notificá-lo no menor prazo possível, apresentando justificativa suficiente e adequada para o não cumprimento do prazo geral.
>
> § 8º Considera-se como conhecimento do incidente, nos termos do caput, o momento a partir do qual o controlador tem razoável grau de certeza da ocorrência do incidente de segurança com dados pessoais, materializada com a ciência pelo Encarregado de Dados ou do responsável pelo canal de comunicação nos termos da Resolução CD/ANPD n. 2/2022.

142. Em relação ao inciso I do caput do art. 6º, houve seis contribuições, todas no sentido de excluir "categoria de dados", de modo a constar apenas a necessidade de se informar a descrição da natureza dos dados pessoais afetados.

143. Quanto ao inciso II do caput do art. 6º, que se refere ao número de titulares afetados, as 26 (vinte e seis) contribuições relacionadas a ele trataram sobre (i) flexibilização da obrigação de informar o número de titulares afetados, em razão de se entender que nem sempre é possível determinar precisamente esse quantitativo.

144. Inclusive, argumenta-se que o § 3º do art. 9º da minuta do regulamento admite essa impossibilidade ao dispor que caso a comunicação direta e individualizada se mostre inviável ou não seja possível determinar, parcial ou integralmente, os titulares afetados, o controlador deverá comunicar a ocorrência do incidente, no prazo e com as informações definidas no caput, pelos meios de divulgação disponíveis.

145. Ainda no inciso II, contribuições argumentaram sobre a (ii) não determinação pela LGPD de obrigatoriedade de indicar do número de crianças, de adolescentes ou de idosos afetados pelo incidente de segurança e impossibilidade de apuração dessa informação a depender do caso; e (iii) a exclusão do termo "idosos", por falta de previsão na LGPD.

146. Além disso, em meio a contribuições referentes a esse inciso II, sugeriu-se abordar a possibilidade de notificações agregadas em caso de violações múltiplas semelhantes a serem comunicadas à ANPD, citando como fundamento o documento Grupo de trabalho do artigo 29.º para a proteção de dados2.

147. Para o inciso III do caput do art. 6º, oito de nove de suas contribuições foram no sentido de reproduzir a redação do inciso III do § 1º do art. 48 da LGPD, de modo a constar o trecho "observados os segredos comercial e industrial". A remanescente buscou incluir disposição no sentido de que o controlador deveria dar validação prévia sobre a aplicabilidade de medidas de segurança e proteção de dados pessoais por operadores, quando estes estivessem envolvidos.

148. Quanto ao inciso IV do caput do art. 6º, houve seis contribuições. Duas foram submetidas com o intuito de excluir a expressão "com identificação dos possíveis impactos aos titulares" e quatro envolvendo a posposição do termo "relevantes" ao termo "riscos", a fim de que o inciso guarde consonância com a LGPD e com a própria redação do Regulamento em questão, ou a expressão "de segurança com dados pessoais" ao termo "incidente", com a ideia de refletir a terminologia incidente de segurança com dados pessoais disposta no artigo 3º, inciso X, da minuta.

149. Em relação ao inciso V do caput do art. 6º, houve quatro contribuições. Duas foram no sentido de incluir a expressão "de segurança com dados pessoais" posposta ao termo "incidente", a título de padronização

terminológica, em razão do art. 3º. Inciso X, da minuta do regulamento. As outras duas sugerem alterar a redação para “os motivos da demora, no caso de a comunicação não ter sido realizada no prazo previsto no caput deste artigo”, que reproduz quase totalmente a redação do texto do art. 48, § 1º, inciso V, da LGPD.

150. Para o inciso VI do caput do art. 6º, houve três contribuições. Foram no sentido de incluir a expressão “de segurança com dados pessoais” posposta ao termo “incidente”, a título de padronização terminológica, em razão do art. 3º, inciso X, da minuta do regulamento. A outra, no sentido de tratar sobre a possibilidade de adoção de medidas futuras no saneamento do incidente, alterando a redação de “serão adotadas” para “poderão ser adotadas” e incluindo “quando cabíveis”, além de complementar o final do dispositivo com “observados os segredos comercial e industrial”.

151. Em relação ao inciso VII do caput do art. 6º, foram onze contribuições. Houve propostas para substituir a expressão "a data e a hora do conhecimento" por "a data da confirmação", excluindo-se o termo “hora”, por dificuldade de aferi-la com precisão, ensejando possível interpretação de violação ao regulamento, além de haver sugestão de incluir "pelo controlador", por se entender que não estaria claro que é o controlador o responsável pela informação; excluir a informação sobre o momento em que se teve conhecimento do incidente; e substituir o termo “do incidente de segurança” por “do incidente de segurança com dados pessoais”, por suposta padronização terminológica com o inciso X do art. 3º da minuta do regulamento, que traz a definição de incidente de segurança com dados pessoais”.

152. Por fim, sugeriu-se acrescentar ao inciso VII do art. 6º o termo "circunstâncias", visto que a ausência de informações acerca das circunstâncias em que o incidente foi conhecido impactaria, em síntese, no marco inicial da contagem do prazo da comunicação (“a partir do conhecimento”) constante dos artigos 6° e 9° da proposta e no juízo de gravidade que a ANPD fará para estabelecer medidas adicionais da comunicação aos titulares.

153. Já sobre o inciso VIII do caput do art. 6º, houve duas propostas. A primeira, a fim de alinhar a redação do inciso ao § 4º do mesmo artigo, busca acrescentar a expressão “ressalvado o previsto no § 4º deste artigo”, que trata da hipótese de o comunicante se tratar de advogado e, por essa razão, dispor de prerrogativa de apresentar procuração em prazo de 15 dias após a comunicação, em respeito ao § 1º do art. 5º da Lei nº 8.906, de 4 de julho de 1994. A segunda trata sobre como se comprova a legitimidade do encarregado quando da comunicação de um incidente, isto é, de que modo a ANPD se certificará de que o encarregado realmente está indicado pelo controlador e, portanto, a comunicação deve ser considerada como válida.

154. Não houve contribuições para o inciso IX do caput do art. 6º.

155. Para o inciso X do caput do art. 6º, houve seis propostas. Duas

foram no sentido de alterar o termo operador por outro agente de tratamento. Outra, no sentido de acrescentar a expressão "e controladores nos casos de compartilhamento de dados pessoais", pois entende que a problemática está na falta de amplitude da comunicação acerca dos agentes de tratamento que podem estar envolvidos no incidente de segurança, podendo vulnerabilizar titulares de dados que estão em outras cadeias de tratamento a qual seus dados são compartilhados. Outras duas, no sentido de que as informações solicitadas deveriam ser esclarecidas em regulamento. A última foi no sentido de acrescer a expressão “envolvido no incidente de segurança com dados pessoais” ao termo operador, por entender que devem ser somente encaminhadas informações sobre o operador que esteja diretamente envolvido no incidente.

156. Dezesseis contribuições foram recebidas para o inciso XI do caput do art. 6º. A maioria foi no sentido ou da inviabilidade ou da inexequibilidade ou da inadequação da comunicação prévia ao titular de dados. Outras apontaram a remissão equivocada ao art. 10, que deveria ser, em verdade, ao art. 9º.

157. Para o inciso XII do caput do art. 6º, houve contribuições sobre suposta necessidade de padronização terminológica na expressão “do incidente”, de modo a constar “incidente de segurança com dados pessoais”, em razão do art. 3º, inciso X, da minuta do regulamento.

158. Quanto ao inciso XIII do caput do art. 6º, foram apresentadas 24 contribuições. A maioria sugere excluir o dispositivo ou por se entender pela desnecessidade dos dados sobre o total de titulares cujos dados são tratados pela organização e na atividade de tratamento afetada pelo incidente ou pela suposta impossibilidade de se obter um número preciso ou, ainda, pela possibilidade de retardar a conclusão da investigação do incidente. Outras contribuições foram no sentido de que esses dados não parecem razoáveis para fins de avaliação do dano ou que não estão associados ao interesse atrelado à comunicação do incidente à ANPD ou que a previsão estaria em desacordo com o art. 48 da LGPD e, por fim, que a ANPD não normatizou, até o momento, os requisitos que devem constar no Registro das Operações de Tratamento de Dados e, por isso, muitas organizações não saberão informar, com precisão, o número solicitado no dispositivo. Houve, igualmente, contribuição no sentido de que a redação deixou de estipular que os dados sobre os quais se refere são os pessoais, considerando o escopo de incidência da norma, e que, ao se utilizar a expressão “organização”, não houve definição do termo na minuta e não seria compatível com os conceitos da LGPD.

159. Quanto ao § 1º do art. 6º, que trata do prazo complementar excepcional para comunicação do incidente à ANPD, foram apresentadas 28 contribuições. Essas sugestões, em sua maioria, estão intrinsecamente ligadas ao caput do art. 6º, que define o prazo para comunicação do incidente. Em regra, as contribuições giram em torno de que o prazo complementar não deve ser excepcional, mas indefinido, ou que a sistemática da comunicação

deva ser em etapas, não em prazo inicial e complementar excepcional; ou, ainda, que o prazo deve ser o mais rápido possível e sem demora injustificada, por prazo máximo de trinta dias úteis ou mesmo quarenta dias úteis. Há contribuição a fim de que se mantenha o prazo praticado atualmente pela ANPD de trinta dias corridos contados a partir da data da comunicação preliminar. Há, também, sugestão no sentido de remover o trecho "uma vez, por igual período". Outro ponto de destaque nas contribuições se dá quanto ao termo inicial de contagem do prazo complementar: que não deve ser do conhecimento do incidente, mas do recebimento da comunicação original ou preliminar ou do despacho de recebimento dessa recepção pela ANPD. Além disso, tendo em vista o período de análise da comunicação pela Autoridade, sugere-se que a ANPD não aprecie o pedido de prorrogação do prazo de complementação da comunicação, e sim que o controlador tenha o prazo prorrogado até decisão da ANPD ou término do prazo. Por fim, houve sugestão de inclusão de um parágrafo ao artigo, com a seguinte redação: Considera-se deferido o pedido de prorrogação não apreciado em até três dias úteis.

160. Para o § 2º do art. 6º, foram nove contribuições. Houve sugestões no sentido de acrescer a expressão "à ANPD" à expressão "A comunicação do incidente de segurança". Houve, também, sugestão no sentido de incluir disposição versando sobre o meio de comunicação do incidente de segurança no caso de indisponibilidade do sistema ou impossibilidade técnica por parte da ANPD e previsão quanto à prorrogação do prazo para a comunicação do incidente. Houve, ainda, sugestão de acréscimo da expressão “com dados pessoais” após o termo "incidente de segurança" para refletir a terminologia inscrita no inciso X do art. 3º da minuta do Regulamento. Por fim, há contribuição no sentido de que o formulário eletrônico disponibilizado pela ANPD não seja a única opção para entrega da comunicação, mas que um formato PDF também seja possível, de modo a agilizar o procedimento para o controlador. Caso o formulário eletrônico seja um instrumento para preenchimento online, o procedimento, em vez de ser simplificado, complicaria a atuação de distintas áreas do controlador envolvidas, além da participação de agentes externos, no fornecimento de informações a serem incluídas no formulário.

161. Para o § 3º do art. 6º, foram quatorze contribuições. Em síntese, as sugestões envolveram a definição do que seria ter legitimidade, quem teria essa legitimidade e como se daria a sua comprovação documental. Uma das contribuições, por exemplo, indica falta de clareza do dispositivo minutado, por entender que a intenção da previsão do § 5º é restringir o rol de pessoas autorizadas a realizar a comunicação de incidentes a pessoas previamente autorizadas. Por isso, entende que terá legitimidade o representante legal do agente de tratamento, mediante demonstração de atendimento aos requisitos constantes no inciso VIII do art. 6º. Dessa maneira, propõe redação para o § 3º no sentido de que a comunicação do incidente de segurança não será admitida quando apresentada em inobservância ao disposto no art. 6º, inciso VIII.

162. Quanto ao § 4º do art. 6º, foram oito contribuições. Boa parte delas foram no sentido de estender a possibilidade de apresentação de instrumento comprobatório de representação/legitimidade em momento posterior à comunicação para além do advogado e sobre dúvidas em que consistiria a legitimidade em si e o documento comprobatório dela, dada a relação do dispositivo com o § 3º.

163. Para o § 5º do art. 6º, foram cinco contribuições. Houve sugestões sobre suposta necessidade de padronização terminológica na expressão “do incidente de segurança”, de modo a constar “incidente de segurança com dados pessoais”, em razão do art. 3º, inciso X, da minuta do regulamento. Houve, também, contribuição no sentido de retirar a possibilidade de "instauração de processo administrativo sancionador para avaliar o descumprimento do previsto nos arts. 6º e 9º deste Regulamento", por entender que a não admissão de uma comunicação de incidente de segurança previstas nos §§ 3º e 4º (por vícios formais – falhas de representação –, nos termos da contribuição) não deve submeter o controlador a um processo sancionatório. Houve, ainda, sugestão indicando falta de clareza no dispositivo minutado, propondo-se redigir "sem prejuízo da possibilidade de instauração de processo administrativo sancionador" por se entender que nem sempre será necessário o processo sancionatório para a apuração da ocorrência de um incidente.

164. Para o § 6º do art. 6º, foram cinco contribuições. Sugeriu-se que o prazo em dobro também deveria ser aplicado ao prazo complementar previsto no § 1º do art. 6º e que a redação da minuta do regulamento não apresenta clareza nesse sentido. Além disso, sugeriu-se a inclusão de entidades de saúde, educação e assistência social no parágrafo 6°, do artigo 6° da Minuta, ou, alternativamente, a inclusão de novo parágrafo garantindo prazo em dobro para as referidas entidades.

165. Para o art. 7º, foram 23 contribuições. Muito se contribuiu no sentido de tratar o processo de comunicação de incidentes como sigiloso por padrão, isto é, que a presunção de publicidade não deveria ser a regra. Sugeriu-se, também, que esteja expresso no dispositivo que o controlador possa requerer motivadamente o sigilo a informações cuja divulgação possa representar violação a segredo comercial ou industrial, ou, ainda, que possa possibilitar a concorrência desleal. Outra sugestão foi no sentido de que deve constar no dispositivo que o controlador deverá, no momento do protocolo, submeter uma versão pública completa e uma versão restrita da comunicação e dos documentos de instrução, ocultando nestes últimos as informações cujo acesso não deverá ser tornado público pela ANPD. Uma das contribuições apontou que o artigo não é claro a respeito do aspecto temporal da solicitação de sigilo ou se a referida solicitação deve ser feita na mesma ocasião da comunicação do incidente de segurança ou, ainda, se há a possibilidade de efetuá-lo de modo apartado, propondo que o sigilo de informações pessoais ou estratégicas de negócios, ou de qualquer outra natureza, devam ser indicadas a qualquer tempo (não somente no âmbito da

comunicação do incidente de segurança). Uma sugestão propôs a inclusão da expressão “ou por contrato”, tendo em vista que o sigilo da informação pode decorrer de estipulação contratual. Outra contribuição foi no sentido de que, considerando que o próprio Estado considera que a manutenção do sigilo de informações relativos à segurança cibernética é imprescindível à segurança do Estado (art. 15 do Decreto nº 10.748, de 16 de junho de 2021), deve-se reconhecer, por simetria, que a eventual publicização de tais informações de entes privados pode ampliar os riscos a que estão expostos, o que pode prejudicar, em última análise, a própria segurança dos dados dos titulares.

166. Para o art. 8º, foram 22 contribuições. Além de proposta de exclusão do dispositivo, houve sugestões a fim de alterar a expressão "a qualquer tempo" por "até o trânsito em julgado da decisão administrativa no processo de comunicação do incidente" ou "durante a análise do incidente". Houve, também, contribuições no sentido de delimitar que o Relatório de Impacto à Proteção de Dados Pessoais (RIPD) deva ser referente à atividade de tratamento afetada pelo incidente; ou que seja previsto que o documento será requerido se o incidente envolver dados pessoais sensíveis, tratamento de alto risco ou fundamentado na base legal do legítimo interesse; ou que seja incluída a expressão "quando cabível", a fim de clarificar que o RIPD nem sempre poderá ser solicitado pela ANPD, em razão da sua própria definição. Houve proposta de alterar a denominação do relatório de tratamento do incidente para relatório de avaliação de incidente de segurança com dados pessoais e de prever o seu conteúdo no regulamento. Houve, ainda, contribuições a fim de que especifique o prazo para solicitação no regulamento, sugerindo-se que seja não inferior a 5 (cinco), 10 (dez) ou 20 (vinte) dias úteis ou no prazo máximo de 60 (sessenta) dias para o envio das informações, ou que se use a expressão "prazo razoável". Ainda quanto ao prazo, há sugestões sobre seu termo inicial, tal como "após o transcurso do prazo previsto para envio de documentos complementares previsto no § 1º do artigo 6º do regulamento" ou " contados a partir do dia seguinte do recebimento da intimação da solicitação pelo controlador". Por fim, houve propostas a fim de expressar ao final do dispositivo "observados os segredos comercial e industrial".

167. Abaixo serão analisadas as principais contribuições apresentadas para cada um dos dispositivos constantes na seção II do capítulo III do regulamento e avaliadas as providências julgadas pertinentes.

Análise:

168. Quanto às contribuições referentes ao caput do art. 6º, considerando os parágrafos 2.3.9 a 2.3.12 da Nota Técnica CGN 36 (3632102), há a fixação de prazo inicial para comunicação à ANPD de 3 (três) dias úteis, sendo previsto prazo para, excepcionalmente, ocorrer a complementação das informações solicitadas, mediante justificativa, no prazo de 20 (vinte) dias úteis, prorrogável uma vez, por igual período, mediante solicitação fundamentada a ser avaliada pela ANPD. Além disso, justifica-se esse prazo

pelas experiências internacionais, quando abordam a complementação das informações. Dessa maneira, há como prover detalhamento técnico, se necessário, em momento posterior. Ademais, nos termos do Relatório de Impacto Regulatório, na definição do que possa ser considerado como "prazo razoável" para comunicação do incidente, verifica-se que essa deverá ocorrer o mais breve possível, considerando, ainda, a necessidade de avaliação prévia por parte do controlador no tocante à classificação do incidente quanto ao risco ou dano relevante que possa ocasionar.

169. Assim, considerando a definição minutada de incidente de segurança com dados pessoais proposta nesta peça processual – qualquer evento adverso confirmado, relacionado à violação das propriedades de confidencialidade, integridade, disponibilidade da segurança de dados pessoais –, quando da ocorrência de um incidente de segurança, deve-se verificar o envolvimento de dados pessoais, pois não necessariamente um incidente envolverá esse tipo de dado. Em caso afirmativo, deve-se avaliar a possibilidade de acarretar risco ou dano relevante aos titulares. Se esses dados forem sensíveis, de crianças, de adolescentes, de idosos, financeiros, de autenticação em sistemas, em larga escala ou protegidos por sigilo judicial, legal ou profissional, então confirma-se a necessidade de comunicação à ANPD.

170. A redação minutada dispõe que a comunicação do incidente de segurança com dados pessoais à ANPD deverá ser realizada no prazo de três dias úteis contados do conhecimento do incidente de segurança, sempre que o incidente possa acarretar risco ou dano relevante aos titulares afetados. É possível interpretar que: i) a contagem iniciar-se-á quando da confirmação do incidente de segurança; ii) a contagem iniciar-se-á quando da confirmação do incidente de segurança com dados pessoais; ou iii) a contagem iniciar-se-á quando da confirmação do incidente de segurança com dados pessoais que possa acarretar risco ou dano relevante aos titulares. A primeira interpretação inclui no prazo de três dias a verificação de que se trata de dados pessoais, sobre a possibilidade de risco ou dano relevante e quanto à natureza e categoria dos dados. Já a segunda exclui desse prazo a verificação de que se trata de dados pessoais, iniciando-se somente quando o controlador constatar a existência de dados pessoais no incidente. A terceira exclui toda a avaliação de modo a se concluir pela comunicabilidade do incidente à ANPD.

171. Dessa forma, a Equipe de Projeto entendeu que se deveria evitar expressões como conhecimento do incidente ou confirmação do incidente, em razão de possíveis ambiguidades.

172. Com isso, elaborou-se nova redação, a fim de clarificar que o prazo começa a ser contado a partir do conhecimento, pelo controlador, de que o incidente afetou dados pessoais. Dessa maneira, esse agente de tratamento disporá de 3 (três) dias úteis para avaliar a possibilidade de riscos e danos relevantes aos titulares dos dados e comunicar à autoridade nacional. Em outras palavras, ao verificar que o incidente afetou dados

pessoais, o controlador deve comunicar o incidente desde que verifique a seguinte condição: possibilidade de o incidente ocasionar risco ou dano relevante aos titulares.

173. Sobre a sugestão no sentido de tornar claro que a comunicação se dará pelo controlador responsável pelo incidente, já que um tratamento de dados pessoais poderá ser realizado por dois controladores, nas hipóteses de co-controladoria, entende-se pela desnecessidade, uma vez que a redação está clara sobre a obrigação por parte do controlador no âmbito do qual se deu o incidente. Assim, a aditamento do termo é desnecessário e gera redundância.

174. Além disso, quanto à sugestão de se excluir a expressão "ressalvada a existência de legislação específica", em razão do disposto no art. 18 do Decreto nº 9.936, de 24 de julho de 2019,[5] respeitante aos procedimentos quanto à ocorrência de vazamento de informações de adimplemento de pessoas naturais cadastradas em bancos de dados para formação de histórico de crédito, nos termos da Lei nº 12.414, de 9 de junho de 2011,[6] manteve-se a redação tal como fora proposta no VOTO Nº 8/2023/DIR/JR/ANPD (4171788). Ademais, substituiu-se a locução conjuntiva temporal "sempre que" pela condicional "desde que" na parte final do caput do art. 6º.

175. Quanto ao Inciso I do caput do art. 6º, não se acatou as contribuições que buscaram excluir o termo “categoria”, pois, no art. 5º da LGPD, incisos I e II, define-se dado pessoal e dado pessoal sensível. A minuta do Regulamento trata essas duas definições como a natureza dos dados. Para classificar os tipos de dados pessoais decorrentes dessas duas naturezas, utiliza-se o termo "categoria" para indicar o tipo de dado, isto é, uma subclassificação. A ANPD, enquanto entidade reguladora e fiscalizadora, detém o poder de regulamentar o modo como os agentes regulados deverão dispor das informações deles requeridas.

176. Em relação ao inciso II do caput do art. 6º, não se deu razão às contribuições a fim de excluir o termo “de idosos”, pois, para além do já fundamentado quanto ao inciso II do art. 5º do Regulamento em causa na seção anterior a esta desta Nota Técnica, acrescenta-se o disposto nos incisos IV, XVI e XIX do art. 55-J da LGPD, pois a ANPD entende que necessita ter a informação sobre violação de dados de pessoas idosas.

177. Quanto à questão sobre número de titulares afetados, entende-se por não acatar as sugestões de modo que o número a ser informado seja aproximado, pois trata-se de um valor de referência. Caso fosse estipulado no regulamento um valor aproximado, deveria ser definida a metodologia de aproximação. Além disso, não há incoerência nesse ponto quanto ao disposto no § 3º do art. 9º da minuta do regulamento, pois esse dispositivo, ao tratar da possibilidade de não ser possível determinar, parcial ou integralmente, os titulares afetados, não trata de quantitativo, mas da identificação do indivíduo.

178. Já sobre a possibilidade de notificações agregadas em caso de violações múltiplas semelhantes a serem comunicadas à ANPD, conforme mencionado pelo Grupo de trabalho do artigo 29 para a proteção de dados, no documento *Guidelines on Personal data breach notification under Regulation* 2016/679, de 2018,[7] é importante ponderar que a comunicação individualizada dos incidentes de segurança com dados pessoais é uma abordagem importante por estar alinhada com os princípios estabelecidos na LGPD, além de ajudar a garantir que os titulares de dados pessoais sejam informados sobre os riscos a que seus dados e, por conseguinte, seu direito à proteção destes, estão sujeitos. Ainda, a comunicação individualizada permite uma maior transparência, por permitir que os titulares de dados tenham ciência exata sobre quais dados foram afetados e quais riscos devem enfrentar, de modo a auxiliá-los a tomar medidas apropriadas para proteger seus próprios interesses, nos termos dos arts. 17 a 22 da LGPD. Ademais, a Lei atribui ao controlador a obrigação de proteger os dados pessoais dos titulares e, por conseguinte, a comunicação de incidentes com dados pessoais de forma agregada pode ser interpretada como uma falta sobre o dever de diligência do controlador, colocando em xeque a confiança dos titulares em relação ao tratamento de seus dados pessoais.

179. Sobre o inciso III do caput do art. 6º, acataram-se as contribuições para a inclusão da expressão "observados os segredos comercial e industrial", de modo a reproduzir a redação do inciso III do § 1º do art. 48 da LGPD. Quanto à contribuição que buscou incluir disposição no sentido de que o controlador deveria dar validação prévia sobre a aplicabilidade de medidas de segurança e proteção de dados pessoais por operadores, quando estes estivessem envolvidos, entende-se, nesse caso, pela desnecessidade de incluir disposição referente a relação entre controlador e operador, pois o operador realiza tratamento de dados em nome do controlador, conforme as instruções deste e contrato entre as partes.

180. Quanto ao inciso IV do caput do art. 6º, não se vislumbrou razão para se excluir a expressão “com identificação dos possíveis impactos aos titulares”, uma vez que para se indicar medidas mitigadoras aos titulares é mister descrever os possíveis impactos.

181. Em relação ao inciso V do caput do art. 6º, acatou-se as sugestões de alterar a redação para “os motivos da demora, no caso de a comunicação não ter sido realizada no prazo previsto no caput deste artigo”, que reproduz quase totalmente a redação do texto do inciso V do § 1º do art. 48 da LGPD.

182. Para o inciso VI do caput do art. 6º, não se acatou as sugestões no sentido de tratar sobre a possibilidade de adoção de medidas futuras no saneamento do incidente, alterando a redação de “serão adotadas” para “poderão ser adotadas” e incluindo “quando cabíveis”, pois o dispositivo reproduz os termos da LGPD.

183. Em relação ao inciso VII do caput do art. 6º, acatou-se as propostas no sentido de se excluir o termo “hora”, por dificuldade de aferi-la com precisão, de se substituir o termo “do incidente de segurança” por "da ocorrência do incidente, quando for possível determiná-la" e de se incluir a expressão "a de seu conhecimento pelo controlador". Ao fim, o inciso serve para que a ANPD tenha informações sobre a data de ocorrência do incidente e a data de seu conhecimento pelo controlador, de modo a se ter ideia do tempo que controladores tem levado para saber da ocorrência de um incidente. Por fim, não se acatou a sugestão de se acrescentar o termo "circunstâncias", pois a equipe de projeto entendeu que as circunstâncias estariam abarcadas pelo inciso XII do art. 6º da minuta pré-consulta pública, ao se tratar da descrição do incidente.

184. Já sobre o inciso VIII do caput do art. 6º, a proposta a fim de alinhar a redação do inciso ao § 4º do mesmo artigo restou prejudicada por causa da alteração que o § 4º sofre após a consulta pública, que será descrita adiante nesta Nota. A outra contribuição quanto a este inciso, sobre como se comprova a legitimidade do encarregado quando da comunicação de um incidente, isto é, de que modo a ANPD se certificará de que o encarregado realmente está indicado pelo controlador e, portanto, a comunicação deve ser considerada como válida, foi tratada pela alteração do § 3º do art. 6º.

185. Para o inciso X do caput do art. 6º, não se acatou as propostas para se alterar o termo operador por outro agente de tratamento, visto que o que se quer saber é a identificação do próprio operador. Quanto a proposta de se acrescentar a expressão "e controladores nos casos de compartilhamento de dados pessoais", entendeu-se que as informações sobre o controlador responsável pelos dados alvo do incidente são as que a ANPD precisa para ter conhecimento sobre o incidente de suas consequências. As demais não foram acatadas porque a equipe de projeto conclui que há clareza no dispositivo de que se trata de operar relacionado ao incidente que está sendo comunicado, quando houver.

186. Em relação ao inciso XI do caput do art. 6º, a CGN concordou quanto à inadequação da comunicação prévia ao titular de dados à ANPD. Por essa razão, exclui-se o inciso e inclui-se parágrafo no art. 9º para tratar do procedimento referente à juntada da declaração de que os titulares foram comunicados no processo de comunicação do incidente.

187. Quanto ao inciso XIII do caput do art. 6º, a equipe de projeto entendeu por excluir o termo "organização" e readequar a redação de modo que o total de titulares informados seja aquele relacionado às atividades de tratamento afetadas pelo incidente.

188. Quanto ao § 1º do art. 6º, que trata do prazo complementar excepcional para comunicação do incidente à ANPD, a equipe de projeto ponderou que, atualmente, a referida excepcionalidade é a regra, isto é, a maioria dos controladores se utiliza do prazo complementar. Por essa razão, entendeu que o termo "excepcionalmente", considerando a vivência prática

da Coordenação-Geral de Fiscalização (CGF), não agregaria valor ao dispositivo, pois que grande parte das comunicações se utilizam dessa medida excepcional. Desse modo, considerando a manutenção dos prazos de comunicação e da sistemática de prazo inicial e prazo complementar, a equipe de projeto entendeu por excluir o termo, de modo a refletir a realidade enfrentada pela CGF. Além disso, entendeu que o marco inicial da contagem do prazo seria mais bem gerenciado pela CGF se fosse a partir da data da comunicação, isto é, de recebimento da comunicação do incidente.

189. Já para o § 2º do art. 6º, a equipe de projeto não viu sentido em se acrescer a expressão "à ANPD" à expressão "A comunicação do incidente de segurança", uma vez que o dispositivo em questão faz parte de seção relativa à comunicação do incidente à ANPD. Por isso, não há necessidade de se reproduzir expressões completas a cada momento em vários dispositivos referentes a um mesmo artigo, pois o artigo é a frase-unidade do contexto, à qual se subordinam parágrafos, incisos, alíneas e itens, e o parágrafo é o complemento aditivo ou restritivo do caput do artigo. Assim, o contexto indica que se trata de comunicação à ANPD. Quanto à sugestão no sentido de incluir disposição versando sobre o meio de comunicação do incidente de segurança no caso de indisponibilidade do sistema ou impossibilidade técnica por parte da ANPD e previsão quanto à prorrogação do prazo para a comunicação do incidente, a equipe de projeto entendeu que, no momento, não seria adequado, pois os processos administrativos eletrônicos no âmbito da ANPD são realizados em sistema informatizado de gestão de processo administrativo eletrônico. No caso de instabilidade, a ANPD avaliará a questão no caso concreto. Em relação à contribuição no sentido de que o formulário eletrônico disponibilizado pela ANPD não seja a única opção para entrega da comunicação, mas que um formato PDF também seja possível, de modo a agilizar o procedimento para o controlador, no momento atual trata-se de formulário eletrônico no formato .docx. Em relação ao § 3º do art. 6º, a fim de dirimir a necessidade de se definir o que seria ter legitimidade, quem teria essa legitimidade e como se daria a sua comprovação documental, a equipe de projeto entendeu por dar nova redação ao dispositivo. A solução proposta pela equipe de projeto é, com fundamento no inciso VIII do art. 5º e no art. 41, ambos da LGPD, e no art. 11 da Resolução CD/ANPD nº 2, de 27 de janeiro de 2022, já deixar explícito no Regulamento que a comunicação de um incidente deverá ser realizada pelo controlador por intermédio do encarregado, por ser a pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador e a ANPD, ou por meio de representante constituído com poderes de representação junto à ANPD. No caso de controladores qualificados como agentes de tratamento de pequeno porte (ATPPs), que não são obrigados a indicar encarregado, somente representante constituído com poderes de representação junto à ANPD poderá encaminhar comunicação de incidente em nome do controlador. Em ambos os casos, deve ser juntado aos autos documento comprobatório da relação com o controlador. Dessa maneira, não haveria dúvidas sobre quem seria pessoas com ou sem legitimidade para comunicar incidentes de segurança com dados pessoais em

nome do controlador.

190. Quanto ao § 4º do art. 6º, a equipe de projeto também atuou no sentido de dar nova redação ao dispositivo, de modo a se coadunar com a nova redação do § 3º. Ademais, a equipe de projeto entendeu pela desnecessidade de se abordar situação de representação de controlador por advogado perante a ANPD, uma vez que o art. 5º da Lei nº 8.906, de 4 de julho de 1994 (Estatuto da Advocacia), já dispõe sobre a capacidade postulatória desse profissional, em juízo ou fora dele. Com isso, as demais contribuições a esse dispositivo restaram prejudicadas.

191. Para o § 5º do art. 6º, a equipe de projeto não acatou as propostas das contribuições, especialmente quanto à sugestão de se retirar a possibilidade de "instauração de processo administrativo sancionador para avaliar o descumprimento do previsto nos arts. 6º e 9º deste Regulamento", por entender que a não admissão de uma comunicação de incidente de segurança previstas nos §§ 3º e 4º, conforme redação pré-consulta pública, por vícios formais, isto é, falhas de representação, não deve submeter o controlador a um processo sancionatório. Ocorre que a hipótese do dispositivo não se deve a vício formal. Deve-se, em verdade, à não comunicação do incidente de segurança, pois a ausência de comprovação da manifestação de vontade do controlador em comunicar o fato descaracteriza o ato de comunicação. Por essa razão é que se iniciará o procedimento de apuração, em vez do procedimento de comunicação. Sem a comprovação da manifestação volitiva do controlador, não há se falar em comunicação do incidente. Quanto à sugestão para incluir o termo “possibilidade" na parte final do dispositivo, de modo a constar "sem prejuízo da possibilidade de instauração de processo administrativo sancionador", com fundamento na falta de clareza do dispositivo minutado e por entender que nem sempre será necessário um processo sancionatório para a apuração da ocorrência de um incidente. A equipe de projeto não acatou pela falta de clareza quanto a seus fundamentos e justificação. No caso, o processo sancionatório não se vale para apurar a ocorrência de um incidente, mas o descumprimento de uma obrigação legal.

192. Em relação ao § 6º do art. 6º, quanto à sugestão de que o prazo em dobro para os ATPPs também deveria ser aplicado ao prazo complementar previsto no § 1º do art. 6º e que a redação da minuta do regulamento não apresenta clareza nesse sentido, a equipe de projeto entendeu haver coerência no raciocínio, uma vez que o prazo para a comunicação de incidente e o prazo para complementar informações sobre esse incidente tem origem no mesmo fato, o incidente. Se o fundamento para se conceder prazo em dobro aos ATPPs é o estabelecimento de um procedimento diferenciado em razão do seu porte e estrutura, não se vislumbra motivos para que, caso haja necessidade de complementação de informações, o prazo para tanto se iguale àquele destinado a controladores com maior capacidade financeira e de atendimento a demandas regulatórias. Quanto à sugestão de inclusão de entidades de saúde, educação e assistência social no parágrafo 6°, do artigo 6° da minuta, ou, alternativamente, a

inclusão de novo parágrafo garantindo prazo em dobro para as referidas entidades, não há abrigo da lei para seu acatamento.

193. Quanto ao art. 7º, a equipe de projeto não acatou nenhuma das contribuições, por entender que não possibilidade legal de se tratar os processos de comunicação de incidentes como sigiloso por padrão, isto é, que a presunção de publicidade não deveria ser a regra. Além disso, a LGPD é bem clara ao buscar proteger os segredos comercial e industrial dos agentes de tratamento.

194. Por fim, para o art. 8º, a equipe de projeto rejeitou todas as propostas, pois visavam ou a exclusão e a limitação do exercício do poder de polícia administrativa pela ANPD, visto que a Lei nº 9.873, de 23 de novembro de 1999, já define o tempo prescricional para a ação punitiva da Administração Pública Federal, direta e indireta, no exercício do poder de polícia, objetivando apurar infração à legislação em vigor. Além disso, rejeitou-se contribuições no sentido de se alterar a redação quanto à solicitação de RIPD, pois a execução dos procedimentos fiscalizatórios deve observar não só o disposto na LGPD sobre o referido relatório, mas também a sua própria regulamentação quanto ao assunto. Quanto aos pedidos de especificação do prazo para envio de informações, a equipe de projeto entendeu que, em atividades de fiscalização, prazos podem variar em conformidade com objeto da fiscalização e o nível de detalhe das informações solicitadas, isto é, conforme o caso concreto.

<u>Proposta de nova redação para os dispositivos em pauta:</u>

195. Após a análise das contribuições acima citadas, é apresentada a nova proposta redacional, sendo que as redações suprimidas se encontram tachadas e as inseridas em negrito, para melhor compreensão da proposta, veja-se:

> Seção II
>
> Da comunicação do incidente **de segurança** à ANPD
>
> Art. 6º A comunicação do incidente de segurança com dados pessoais à ANPD deverá ser realizada pelo controlador~~,~~ no prazo de três dias úteis, ressalvada a existência de legislação específica, contados do conhecimento **pelo controlador** ~~do incidente de segurança~~ **de que o incidente afetou dados pessoais**, ~~sempre~~ **desde** que o incidente possa acarretar risco ou dano relevante aos titulares afetados, ~~devendo~~ **e deverá** conter as seguintes informações:
>
> I - a descrição da natureza e da categoria de dados pessoais afetados;
>
> II - o número de titulares afetados, discriminando, quando aplicável, o número de crianças, de adolescentes ou de idosos;
>
> III - as medidas de segurança para a proteção dos dados pessoais adotadas antes e após o incidente**, observados os segredos comercial e industrial**;

IV - os riscos relacionados ao incidente com identificação dos possíveis impactos aos titulares;

V - **os motivos da demora, no caso de a comunicação não** ter sido ~~os motivos da comunicação do incidente não ter sido~~ realizada no prazo **previsto no *caput* deste artigo**~~, se for o caso~~;

VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do incidente sobre os titulares;

VII - a data ~~e a hora~~ **da ocorrência do incidente, quando possível determiná-la, e a de seu conhecimento pelo controlador**~~do conhecimento do incidente de segurança~~;

VIII - os dados do encarregado~~, quando aplicável,~~ ou **de quem represente o controlador** ~~do, comunicante, acompanhado, nesta hipótese, de procuração ou outro instrumento com poderes para representar o controlador junto à ANPD~~;

IX - ~~os dados de~~ **a** identificação do controlador e, se cabível, declaração de tratar-se de agente de tratamento de pequeno porte;

X - ~~as informações~~ **a identificação do** ~~sobre o~~ operador, quando aplicável;

~~XI - a declaração de que foi realizada a comunicação aos titulares, nos termos do art. 10 deste Regulamento;~~

~~XII~~ **XI** - a descrição do incidente, incluindo a causa principal, caso seja possível identificá-la; e

~~XIII~~ **XII** - o total de titulares cujos dados são tratados ~~pela organização e~~ na**s** atividade**s** de tratamento afetada**s** pelo incidente.

§ 1º ~~Excepcionalmente, a~~**A**s informações poderão ser complementadas, no prazo de vinte dias úteis, a contar **da data da comunicação** ~~do momento em que o controlador tomou conhecimento do incidente~~, prorrogável uma vez, por igual período, mediante solicitação fundamentada a ser avaliada pela ANPD.

§ 2º A comunicação do incidente de segurança deverá ocorrer por meio de formulário eletrônico, disponibilizado pela ANPD.

~~§ 3º A comunicação do incidente de segurança não será admitida quando apresentada por pessoa sem legitimidade.~~

§ 3º A comunicação do incidente de segurança deverá ser realizada pelo controlador, mediante seu encarregado, acompanhada de documento comprobatório de vínculo contratual, empregatício ou funcional, ou por meio de representante constituído, acompanhada de instrumento com poderes de representação junto à ANPD.

~~§ 4º Caso o controlador seja representado por advogado, este poderá efetuar a comunicação sem procuração, obrigando-se a apresentá-la no prazo de até quinze dias úteis, a contar da data da comunicação, sob pena desta não ser admitida.~~

§ 4º Os documentos de que trata o § 3º deverão ser apresentados

em até quinze dias úteis contados da comunicação do incidente, independentemente de notificação ou exigência, sob pena de inadmissão da comunicação.

§ 5º Nas hipóteses de não admissão da comunicação do incidente previstas no~~s~~ ~~§§ 3º e~~ 4º, a ANPD poderá apurar a ocorrência do incidente de segurança por meio do procedimento de apuração de incidente de segurança, sem prejuízo da instauração de processo administrativo sancionador para avaliar o descumprimento do previsto nos arts. 6º e 9º deste Regulamento.

§ 6º O**s** prazo**s** constante**s** no *caput* deste artigo **e no §1º** conta-se em dobro para os agentes de pequeno porte, nos termos do disposto no Regulamento de aplicação da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) aos agentes de tratamento de pequeno porte, aprovado pela Resolução CD/ANPD nº 2, de 27 de janeiro de 2022.

Art. 7º Cabe ao controlador solicitar à ANPD, de maneira fundamentada, o sigilo de informações protegidas por lei, indicando aquelas cujo acesso deverá ser restringido, a exemplo das relativas à sua atividade empresarial cuja divulgação possa representar violação de segredo comercial ou industrial.

Art. 8º A ANPD poderá, a qualquer tempo, solicitar informações adicionais ao controlador, referentes ao incidente de segurança, inclusive o registro das operações de tratamento dos dados pessoais afetados pelo incidente, o relatório de impacto à proteção de dados pessoais (RIPD) e o relatório de tratamento do incidente, estabelecendo prazo para o envio das informações.

Regulamento - Cap. III - Seção III - Da comunicação do incidente de segurança ao titular de dados pessoais:

196. A minuta do regulamento colocada em consulta pública tem o seguinte texto para essa seção:

Seção III

Da comunicação de incidente ao titular de dados pessoais

Art. 9º A comunicação do incidente de segurança com dados pessoais ao titular deverá ser realizada pelo controlador, no prazo de três dias úteis contados do conhecimento do incidente de segurança, sempre que o incidente possa acarretar risco ou dano relevante aos titulares afetados, e deve conter as seguintes informações:

I - a descrição da natureza e da categoria de dados pessoais afetados;

II - os riscos ou impactos ao titular;

III - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do incidente, quando cabíveis;

IV - a data do conhecimento do incidente de segurança; e

V - o contato para obtenção de informações e dados do encarregado,

quando aplicável.

§ 1º A comunicação do incidente aos titulares de dados deverá atender aos seguintes critérios:

I - fazer uso de linguagem simples e de fácil entendimento; e

II - ocorrer de forma direta e individualizada, caso seja possível identificá-los.

§ 2º Considera-se comunicação de forma direta e individualizada aquela realizada pelos meios usualmente utilizados pelo controlador para contatar o titular, tais como, telefone, e-mail, mensagem eletrônica ou carta.

§ 3º Caso a comunicação direta e individualizada se mostre inviável ou não seja possível determinar, parcial ou integralmente, os titulares afetados, o controlador deverá comunicar a ocorrência do incidente, no prazo e com as informações definidas no *caput*, pelos meios de divulgação disponíveis, tais como na sua página na Internet, em aplicativos, em suas mídias sociais e em canais de atendimento ao titular, de modo que a comunicação permita o conhecimento amplo, com direta e fácil visualização pelo período de, no mínimo, seis meses.

§ 4º A ANPD determinará que o controlador faça nova comunicação, caso a primeira não contenha todas as informações necessárias ou tenha se utilizado de meios inadequados, ou ainda que comunique o incidente de segurança ao titular, caso a comunicação não tenha sido realizada.

§ 5º Poderá ser considerada boa prática para fins do disposto no art. 52, §1º, IX da LGPD, a inclusão na comunicação ao titular de recomendações aptas a reduzir os efeitos do incidente.

§ 6º O prazo constante no *caput* deste artigo conta-se em dobro para os agentes de pequeno porte, nos termos do disposto no Regulamento de aplicação da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) aos agentes de tratamento de pequeno porte, aprovado pela Resolução CD/ANPD nº 2, de 27 de janeiro de 2022.

Contribuições recebidas:

197. Das contribuições apresentadas para este capítulo, destacam-se, pelo volume e relevância, as seguintes sugestões:

198. Em relação ao caput do art. 9º, as propostas condensaram-se, em maioria, na relação entre o prazo de 03 (três) dias úteis estabelecido no Regulamento e a necessidade de promoção de um razoável equilíbrio entre a contagem e as investigações internas sobre o incidente.

199. Segundo os participantes, há evidências de que a ANPD está adotando o caminho de exigir a comunicação de incidentes confirmados ao definir incidente de segurança com dados pessoais como qualquer evento adverso confirmado, conforme inciso X do art. 3º da minuta, bem como nas

Orientações sobre comunicação de incidente de segurança, de 20 de abril de 2023.

200. Sem prejuízo dessa compreensão, foram significativas as recomendações no sentido de que o Regulamento deve reforçar essa tônica na redação do art. 9º, para não haver dúvidas de que o prazo para comunicação não comece a contar enquanto o controlador estiver na fase de apuração interna sobre se houve ou não incidente. Ou seja, a redação do art. 9º é confusa, tendo em vista que o "mero conhecimento" do incidente não deveria deflagrar o dever de comunicação, senão a confirmação da existência de um incidente qualificado, isto é, capaz de gerar risco ou dano relevante aos titulares afetados.

201. Assim, entendem que a redação do caput do art. 9º deve ser modificada para eliminar margens interpretativas distintas daquela acima, esclarecendo que o termo inicial do prazo de comunicação é o momento da confirmação, após avaliação da gravidade do incidente. Por isso, entendem que a redação do caput do art. 9º deve ser modificada para sanar margem interpretativa diferente da acima, esclarecendo o termo inicial do prazo de comunicação sendo o momento da confirmação, pós-avaliação, da gravidade do incidente. Isto se deve ao fato de que, na maioria dos incidentes de segurança envolvendo dados pessoais, conforme indicado pelos participantes, é improvável que se possa avaliar de forma apropriada, em apenas 3 (três) dias úteis a partir do momento em que se tem conhecimento do incidente, se existe risco ou dano relevante aos titulares afetados. Isso ocorre porque suspeitas de incidentes e incidentes precisam ser devidamente tratados, identificados e confirmados pelos controladores antes de qualquer comunicação, especialmente aos titulares dos dados. Isso é feito como parte da responsabilidade corporativa e da proteção dos próprios titulares.

202. Nesses moldes, as 47 contribuições relativas ao prazo de comunicação previsto no caput do art. 9º apresentaram as ressalvas abaixo:

> I - Improvável cumprimento do rol de informações previsto no art. 9º junto aos titulares de dados, ou risco de provê-las de forma imprecisa ou extremamente vaga, diante da contagem do prazo se dar do incidente e do prazo estabelecido;
>
> II - Perigo de fadiga de informação desnecessária aos titulares de dados em razão do início da contagem do prazo se dar do conhecimento do incidente e do curto prazo estipulado, ainda mais para casos em que se conclua, posteriormente, que não havia risco ou dano relevante ou se medidas adotadas pelo controlador, após o evento, retiraram a possibilidade de acarretar risco ou dano relevante;
>
> III - Eventual notificação excessiva de incidentes com dados pessoais poder culminar em um resultado maléfico para a confiança social;

IV - Diferença entre a confirmação de um incidente para a efetiva avaliação e confirmação de risco ou dano relevante aos titulares afetados.

V - Necessidade de comunicar os titulares antes da ANPD poder representar um risco ou até mesmo agravar o incidente, em alguns casos, como naqueles em que o incidente tenha sido causado por agente malicioso. Nesses casos, segundo os participantes, a resposta deveria ser coordenada com a ANPD e demais autoridades competentes, a fim de determinar se é adequado comunicar aos titulares, de que maneira e quando.

203. Assim, foram sugeridos, dentre outros pontos, os seguintes:

I - Alteração do prazo de comunicação ao titular, seguindo o mesmo prazo estipulado à ANPD, sendo que, em caso de dados pessoais sensíveis, o prazo poderá ser reduzido, devido à gravidade do caso;

II - Extensão do prazo de notificação para 4 (quatro), 5 (cinco), 7 (sete), 10 (dez), 15 (quinze), 20 (vinte) ou 30 (trinta) dias úteis;

III - Comunicação aos titulares posteriormente à comunicação à ANPD;

IV - Alteração do dispositivo para estabelecimento de sistemática de notificação prévia à ANPD, no prazo de 3 (três) dias úteis do conhecimento do incidente, mas a comunicação efetiva, se e quando confirmado risco ou dano relevante, à ANPD e aos titulares afetados, sem demora indevida, em até 30 (trinta) dias contados da prévia, prorrogáveis por mais 30 (trinta) dias;

V - Alteração do dispositivo para estabelecimento de sistemática de comunicação aos titulares, a depender do caso concreto, de forma “imediata e simplificada” com o objetivo de minimizar os efeitos do incidente, a exemplo de possíveis fraudes na ocorrência de vazamento de dados de cartão de crédito, devendo ser realizada de forma completa no prazo de “até 5 dias úteis”;

VI - Alteração do dispositivo para estabelecimento de sistemática de comunicação aos titulares posterior à comunicação à ANPD, na medida que, em sendo simultânea ou prévia à da ANPD, é possível que a apuração ainda esteja em andamento pelo Controlador e eventual comunicação preliminar e incompleta aos titulares possa gerar fadiga e quebra de confiança dos titulares;

VII - Estabelecimento de prazos separados entre a comunicação para a ANPD e para o titular e um prazo mais longo para notificação deste, de modo que seja determinado em dobro àquele previsto para fins de comunicação à ANPD. Ademais, segundo os participantes, sua contagem deve ser iniciada a partir da constatação, pelo controlador, de que o incidente de segurança com dados pessoais pode gerar risco ou dano relevante aos titulares afetados, termo a quo definido pela própria lei no caput do art. 48. da LGPD;

VIII - Alteração da redação do artigo 9º, caput, para a seguinte: "Art. 9º A comunicação do incidente de segurança com dados pessoais ao titular deverá ser realizada pelo controlador, se adequado e conforme determinação da ANPD, no prazo de três dias úteis contados da determinação da ANPD, sempre que o incidente possa acarretar risco ou dano relevante aos titulares afetados, e deve conter as seguintes informações".

204. Em relação aos incisos e parágrafos do art. 9º, foram apresentadas algumas problemáticas e sugestões.

205. Dentre as problemáticas apontadas, foram mais numerosas e/ou relevantes as seguintes:

I - Necessária inclusão da figura e obrigação de comunicação do operador, que atualmente está com prazo previsto apenas em contrato, sem regulamentação específica;

II - Possibilidade de gerar uma sobrecarga de atendimento direcionada ao encarregado em virtude da redação do inciso V.

III - O destaque durante 6 (seis) meses no site de uma instituição poderá afetar sua reputação que resultará em problemas financeiros que consequentemente poderá até refletir no número de funcionários - poderia ser inserido um prazo de 3 (três) até 6 (seis) meses a depender da situação em que o incidente ocorreu.

IV - Nem sempre quando se identifica um titular é possível contatá-lo para fins de comunicação do incidente de forma direta e individualizada tal como previsto no inciso I, do § 1º.

V - O § 3º impõe que a comunicação em meios de divulgação ocorra se a comunicação se mostrar inviável ou caso não seja possível ao controlador determinar a totalidade dos titulares afetados no incidente. Em sua literalidade, o artigo implica na obrigação de realização da comunicação pública sempre que o controlador não consiga determinar a

totalidade dos titulares afetados no incidente, dentro do prazo de 3 (três) dias. Segundo os participantes, dada a natureza do processo de tratamento de incidentes de segurança, e as incertezas envolvidas, a comunicação pública pode se tornar a regra e não uma exceção. Havendo a comunicação pública, dispensa-se a comunicação individual ao titular, que tende a ser mais efetiva. Por outro lado, em contraste ao RGPD, que possibilita a realização de uma comunicação pública em razão de um esforço desproporcional, a redação proposta exige a comprovação de uma inviabilidade da realização da comunicação individual. A comprovação da inviabilidade, que pode decorrer de diversos fatores, pode ser complexa e onerosa ao agente de tratamento de dados.

206. Quanto às sugestões de ajustes redacionais, apresentaram-se as em maior volume e/ou relevância as seguintes:

I - Alteração do inciso III para a seguinte redação: “III - a indicação de que medidas de segurança foram adotadas para reverter ou mitigar os efeitos do incidente de segurança com dados pessoais, quando cabíveis;”

II - Ajuste de redação do inciso II para delimitar o objeto da comunicação, adotando-se a seguinte redação: “II - os riscos relacionados ao incidente, com identificação dos possíveis impactos aos titulares;”

III - Alteração do inciso III para a seguinte redação: “III - a indicação de que medidas de segurança foram adotadas para reverter ou mitigar os efeitos do incidente de segurança com dados pessoais, quando cabíveis, observados os segredos comercial e industrial;”

IV - Ajuste de redação do inciso V para “V - contato para obtenção de informações e dados de contato do encarregado, quando aplicável.”

V - Ajuste de redação do inciso II, do § 1º para a seguinte redação: “II - ocorrer de forma direta e individualizada, caso seja possível identificá-los e contatá-los.”

VI - Ajuste de redação do inciso II, do § 1º para fazer constar o trecho “(...) ou por meio de outros canais utilizados pelo controlador.”

VII - Ajuste de redação do inciso II do § 1º para: “II - ocorrer, preferencialmente, de forma direta e individualizada, caso seja possível identificá-los e contatá-los, salvo se o controlador decidir por outro meio de comunicação mais eficiente."

VIII - Redução no prazo de 6 (seis) meses para divulgação da comunicação previsto no § 3º;

IX - Alteração da redação do § 5º para a seguinte redação: “Poderá ser considerada boa prática para fins do disposto no art. 52, § 1º, IX, da LGPD, a inclusão na comunicação ao titular de recomendações aptas a reduzir os efeitos do incidente de segurança com dados pessoais e circunstância atenuante, nos termos do art. 13, II, da Resolução CD/ANPD nº 4/2023, que institui o Regulamento de Dosimetria e Aplicação de Sanções Administrativas."

207. Nestes mesmos moldes, foram sugeridas as seguintes inclusões na minuta:

I - Inclusão de um parágrafo com a seguinte redação “§ xº - Não será necessário comunicar aos titulares o incidente de segurança com dados pessoais ao qual o controlador não tenha dado causa, hipótese em que o controlador poderá informar as pessoas impactadas a respeito da situação e os riscos dela decorrentes.”

II - Inclusão de redação que diferencie os critérios que geram o dever de notificação para a autoridade nacional e para os titulares, considerando que as comunicações cumprem propósitos distintos. Ou seja, possibilidade de incluir exceções para que a notificação possa comprometer investigação pela ANPD ou autoridade competente ou, ainda, caso o controlador de dados, ao tomar conhecimento do incidente, tenha tomado medidas que sejam suficientes para impedir que riscos para o titular de dados se materializem.

III - Inclusão de um parágrafo a respeito da não necessidade de comunicação ao titular se os riscos foram neutralizados. Segundo os participantes, se o controlador implementou e aplicou medidas de segurança técnicas e administrativas adequadas aos dados pessoais afetados pelo incidente, especialmente aquelas medidas que tornam os dados pessoais ininteligíveis para qualquer pessoa que não esteja autorizada a acessá-los, como, por exemplo, a encriptação de dados; ou nas situações em que o controlador adotou medidas de segurança técnicas e administrativas subsequentes ao incidente que asseguram que o risco ou dano relevante aos titulares não tenha mais probabilidade de se concretizar.

IV - Inclusão de um parágrafo com a seguinte redação “§ xº - Em havendo relação comercial com operador, e caso o incidente tenha advindo deste, o prazo para comunicação ao controlador será de 2 (dois) dias úteis."

V - Inclusão de um inciso com a seguinte redação “VI - Recomendações ao titular para reduzir os efeitos do incidente, sempre que possível”

VI - Inclusão de parágrafo com a seguinte redação “O prazo de que trata o caput deste artigo não contempla o prazo inicial necessário para que o controlador investigue a ocorrência ou não do fato.";

VII - Inclusão de parágrafo com a seguinte redação “§ xº A avaliação de risco e dano relevante deve ser realizada pelo controlador em prazo razoável e sem atrasos injustificáveis a partir do momento da identificação do incidente de segurança”.

VIII - Inclusão dos seguintes parágrafos: (i) “§ xº Considera-se como alto risco de dano relevante aos titulares a definição da regulamentação própria da ANPD sobre o tema”, (ii) “§ xº Em caso de impossibilidade de comunicar o incidente no prazo estipulado no caput, o agente de tratamento deverá notificá-lo no menor prazo possível, apresentando justificativa suficiente e adequada para o não cumprimento do prazo geral.” e (iii)“ § xº Considera-se como conhecimento do incidente, nos termos do caput, o momento a partir do qual o controlador tem razoável grau de certeza da ocorrência do incidente de segurança envolvendo dados pessoais, materializada com a ciência pelo Encarregado de Dados ou do responsável pelo canal de comunicação nos termos da Resolução CD/ANPD nº 2/2022.”

IX - Inclusão de parágrafo com a seguinte redação “§ xº A comunicação ao titular não será requerida se ao menos uma destas condições se manifestar: I - o controlador implementou medidas de segurança técnicas e administrativas adequadas, e estas medidas foram aplicadas aos dados pessoais afetados, de forma a tornar tais dados ininteligíveis a qualquer pessoa ou agente que não está autorizado a acessá-los; ou II - o controlador tomou medidas que garantam que o risco ou dano relevante descritos no caput tenha baixa possibilidade de concretização”.

Análise:

208. Quanto às 47 contribuições relativas ao prazo de comunicação previsto no caput do art. 9º, cumpre frisar que a minuta do Regulamento estabelece a fixação de prazo inicial para comunicação à ANPD de 3 (três) dias úteis, sendo previsto prazo para, excepcionalmente, ocorrer a complementação das informações solicitadas, mediante justificativa, no prazo de 20 (vinte) dias úteis, prorrogável uma vez, por igual período, mediante

solicitação fundamentada a ser avaliada pela ANPD.

209. Assim, é importante esclarecer nesse sentido que, em consonância com o Relatório de Análise de Impacto Regulatório, verifica-se a necessidade de avaliação prévia por parte do controlador no tocante à classificação do incidente quanto ao risco ou dano relevante que possa ocasionar.

210. Com isso, o prazo atribuído à comunicação ao titular deve ser contado a partir da tomada de conhecimento pelo controlador de que o incidente afetou dados pessoais, restando ao controlador avaliar a possibilidade de risco ou dano relevante aos titulares e comunicá-los no prazo razoável estabelecido pela ANPD.

211. Logo, a equipe de projeto entendeu não haver dúvidas de que o prazo para comunicação não começa a contar enquanto o controlador estiver na fase de apuração interna sobre se houve incidente, ou não, motivo pelo qual nenhuma das 47 (quarenta e sete) contribuições acima citadas foi deferida.

212. Quanto às contribuições referentes aos incisos e parágrafos do art. 9º, impende destacar que não houve contribuições relativas ao inciso I, e a única contribuição referente ao inciso IV foi indeferida pela equipe de projeto.

213. Isso porque o conhecimento do incidente de segurança com dados pessoais se dá em qualquer evento adverso confirmado, relacionado à violação das propriedades de confidencialidade, integridade e disponibilidade da segurança de dados pessoais, motivo pelo qual o conhecimento previsto no inciso IV refere-se à confirmação de incidente de segurança com dados pessoais.

214. Por sua vez, três contribuições propuseram ajuste no inciso II para delimitar o objeto da comunicação, sugerindo a seguinte redação: “II - os riscos relacionados ao incidente, com identificação dos possíveis impactos aos titulares;”

215. Considerando que a proposta parece mais completa que o dispositivo da minuta, além de esclarecer que a referência se faz aos riscos relacionados ao incidente, a equipe de projeto concordou com a inclusão da redação acima proposta.

216. Nesse esteio, três contribuições propuseram alteração do inciso III para a seguinte redação: “III - a indicação de que medidas de segurança foram adotadas para reverter ou mitigar os efeitos do incidente de segurança com dados pessoais, quando cabíveis, observados os segredos comercial e industrial;”.

217. Tais sugestões foram indeferidas pela equipe de projeto à medida que propõem restringir o direito de acesso do titular a quais medidas foram tomadas mediante a ocorrência do incidente de segurança, o que deve

ser privilegiado pelo Regulamento, e não suprimido.

218. Outrossim, uma contribuição propôs ajuste de redação do inciso V para "V - contato para obtenção de informações e dados de contato do encarregado, quando aplicável." - a qual não foi aceite pela equipe de projeto nos moldes propostos.

219. Todavia, para proporcionar maior clareza à redação, propõe-se a seguinte redação:

> V - o contato para obtenção de informações e, **quando aplicável, os** dados do encarregado~~, quando aplicável~~.

220. Quanto ao § 1º, as seis contribuições oferecidas se concentraram nos ajustes redacionais relativos ao inciso II do § 1º para propositura da seguinte redação: "II – ocorrer, preferencialmente, de forma direta e individualizada, caso seja possível identificá-los e contatá-los, salvo se o controlador decidir por outro meio de comunicação mais eficiente." e não houve contribuição para o §2º.

221. Relativamente às seis contribuições supracitadas, a equipe de projeto entendeu que a redação proposta, dentre outros pontos, inverte a lógica da ANPD de privilegiar a comunicação ao titular de forma direta e individualizada em alternativa à comunicação coletiva, motivo pelo qual indeferiu as sugestões.

222. Quanto ao § 2º, não houve contribuições à medida que restou esclarecido que o rol de meios sugeridos não é taxativo.

223. Quanto ao § 3º, quinze contribuições questionaram o prazo de 6 (seis) meses para divulgação da comunicação, sugerindo, em rol não taxativo, redução para 1 (um), 2 (dois), 3 (três) meses e até quanto a não determinação de prazo, conforme redação proposta abaixo:

> "Art. 9º...
>
> (...)
>
> *§ 3º Se a comunicação direta e individualizada se mostrar impraticável ou não for possível determinar, em parte ou no todo, os titulares dos dados afetados e se o incidente for considerado grave nos termos do art. 19, o controlador deve comunicar a ocorrência do incidente, no prazo e com as informações definidas no caput, por meio dos meios de divulgação disponíveis, como em seu site, em aplicativos, em suas redes sociais e nos canais de atendimento , de forma que a comunicação permita amplo conhecimento, com visualização direta e fácil por um período proporcional à gravidade do incidente."*

224. A equipe de projeto entendeu que a ampla divulgação pelo período estipulado não configura eventual penalidade à medida que o dispositivo facultou, em rol não taxativo, a escolha pela comunicação do incidente grave em qualquer meio de divulgação disponível. Assim, foram realizados apenas os ajustes ortográficos, nos moldes abaixo:

> §3º Caso a comunicação direta e individualizada se mostre inviável ou não seja possível determinar, parcial ou integralmente, os titulares afetados, o controlador deverá comunicar a ocorrência do incidente, no prazo e com as informações definidas no caput, pelos meios de divulgação disponíveis, tais como **seu sítio eletrônico**, aplicativos, suas mídias sociais e canais de atendimento ao titular, de modo que a comunicação permita o conhecimento amplo, com direta e fácil visualização, pelo período de, no mínimo, **três** meses.

225. Quanto ao § 4º, oito contribuições propuseram ajustes redacionais especialmente quanto ao momento e a forma definidos pela ANPD para que o controlador faça uma nova comunicação, a fim de haver previsibilidade aos controladores. Segue proposta apresentada:

> "§ 4º A ANPD determinará que o controlador faça nova comunicação no prazo de até 20 dias úteis a contar da comunicação caso a primeira não contenha todas as informações necessárias ou tenha se utilizado de meios inadequados."

226. A justificativa para a sugestão da redação acima - quanto ao prazo de até 20 (vinte) dias úteis a contar da comunicação - é estar em consonância com a comunicação complementar prevista no § 1º do art. 6º. Além disso, conforme se observa, fora suprimida a expressão "ou ainda que comunique o incidente de segurança ao titular, caso a comunicação não tenha sido realizada", tendo em vista que o art. 16 da presente minuta prevê o mesmo conteúdo.

227. A despeito das argumentações trazidas, a equipe de projeto entendeu pelo indeferimento da redação proposta nas oito contribuições, mas considerou a necessidade de clarificar o disposto no teor do § 4º, motivo pelo qual propôs a seguinte alteração de redação para esse parágrafo, renumerado para 6º:

> §6º A ANPD poderá determinar ao controlador que comunique o incidente de segurança ao titular quando não o houver comunicado ou a comunicação realizada **tenha sido inadequada**.

228. Quanto ao § 5º, dezenove contribuições se manifestaram propondo a substituição do termo "poderá ser" para "será".

229. Ademais, uma contribuição refere-se à inclusão do § 5º como uma das informações obrigatórias ao titular na comunicação de incidente pelo controlador e propõe a inclusão de novo inciso no artigo nos seguintes termos: "VI - Recomendações ao titular para reduzir os efeitos do incidente, sempre que possível".

230. Considerando o compilado de sugestões sobre este ponto, a equipe de projeto entendeu impertinente a inclusão do inciso VI nos moldes propostos e eventual alteração do § 5º à medida que há que se verificar questões concernentes ao conteúdo das recomendações no caso concreto antes de considerar efetivamente como boas práticas. Apenas renumerou-se esse parágrafo para § 7º.

231. No que tange ao § 6º, apenas foi renumerado para 8º.

232. Por fim, relativamente às oito contribuições que sugeriram incluir exceções para a comunicação do titular no caso que a comunicação possa comprometer investigação pela ANPD ou autoridade competente, ou, ainda, caso o controlador de dados, ao tomar conhecimento do incidente, tenha tomado medidas que sejam suficientes para impedir que riscos para o titular de dados se materializem, a CGN entende, conforme exposto na seção referente ao art. 4 e 5º desta Nota Técnica, que a LGPD não oferece margem para se isentar comunicação ao titular, visto que cabe à ANPD verificar a gravidade de incidentes comunicados a si, mediante juízo que avaliará eventual comprovação de medidas que tornem os dados afetados pelo incidente ininteligíveis, nos termos dos §§ 2º e 3º do art. 48 da LGPD, podendo, inclusive, determinar adoção de providências, tal como a ampla divulgação do fato em meios de comunicação, o que supera a própria comunicação individualizada ao titular. No entanto, a CGN compreendeu que a realidade pode impor uma postergação da comunicação ao titular em razão de recomendação de autoridade policial ou judiciária, em razão de investigação criminal sobre a ocorrência do incidente. Por esse motivo, elaborou-se os seguintes dispositivos para a minuta:

> §4º O controlador deverá juntar ao processo de comunicação do incidente uma declaração de que foi realizada a comunicação aos titulares, constando os meios de comunicação ou divulgação utilizados, em até três dias úteis, contados do término do prazo de que trata o *caput* deste artigo.
>
> § 5º Em caso de recomendação de autoridade policial ou judiciária para que os titulares não sejam comunicados no prazo de que trata o *caput* deste artigo, por causa de investigação criminal, o controlador deverá juntar ao processo de comunicação do incidente:
>
> I - documento comprobatório emitido pela autoridade policial ou judiciária, com indicação do número do processo ou do procedimento investigatório;
>
> II - a declaração de que trata o § 4º deste artigo em até 3 (três) dias úteis contados do término da recomendação de não comunicação.

233. Dessa maneira, conforme já registrado alhures, os §§ 4º a 6º foram remunerados de 6º a 8º. Além disso, em tempo, registra-se que o caput do art. 9º foi ajustado nos mesmos termos que o caput do art. 6º, conforme justificativa anteriormente. Igualmente, foram incluídos todos os incisos do § 1º do art. 48 da LGPD, com as devidas adaptações oriundas dos incisos do art. 6º, por se tratar de elementos mínimos a serem comunicados tanto à ANPD quanto ao titular, conforme justificação já apresentada anteriormente. Por isso, os demais incisos foram renumerados.

234. Ressalva-se, novamente, que a CGN manifesta reservas quanto à menção do conteúdo disposto no inciso II do § 1º do art. 48, informações

sobre os titulares envolvidos, na comunicação individualizada aos titulares, por entender que esse inciso se refere sobre a identificação dos titulares e não caberia informar a um titular informações sobre os demais, mas somente à ANPD. Por essa razão, surge uma dúvida jurídica a ser dirimida pela PFE/ANPD quanto à possibilidade de não inclusão desse conteúdo na comunicação ao titular, em que pese conste da LGPD como elemento mínimo a ser mencionado nessa comunicação.

Proposta de nova redação para os dispositivos em pauta:

235. Após a análise das contribuições acima citadas, é apresentada a nova proposta redacional, sendo que as redações suprimidas se encontram tachadas e as inseridas em negrito, para melhor compreensão da proposta:

> Seção III
>
> Da comunicação do incidente **de segurança** ao titular de dados pessoais
>
> Art. 9º A comunicação do incidente de segurança com dados pessoais ao titular deverá ser realizada pelo controlador~~,~~ no prazo de três dias úteis contados do conhecimento **pelo controlador** ~~do incidente de segurança~~ **de que o incidente afetou dados pessoais, desde** ~~sempre~~ que o incidente possa acarretar risco ou dano relevante aos titulares afetados, ~~e, devendo~~ **e deverá** conter as seguintes informações:
>
> I - a descrição da natureza e da categoria de 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;**
>
> ~~II~~**IV - ~~os riscos ou impactos ao titular~~ os riscos relacionados ao incidente com identificação dos possíveis impactos aos titulares;**
>
> **V - os motivos da demora, no caso de a comunicação não ter sido feita no prazo do *caput* deste artigo;**
>
> ~~II~~**VI** - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do incidente, quando cabíveis;
>
> ~~IV~~**VII** - a data do conhecimento do incidente de segurança; e
>
> ~~V~~**VIII** - o contato para obtenção de informações e**, quando aplicável, os** dados do encarregado~~, quando aplicável~~.
>
> § 1º A comunicação do incidente aos titulares de dados deverá atender aos seguintes critérios:
>
> I - fazer uso de linguagem simples e de fácil entendimento; e
>
> II - ocorrer de forma direta e individualizada, caso seja possível identificá-los.
>
> § 2º Considera-se comunicação de forma direta e individualizada

aquela realizada pelos meios usualmente utilizados pelo controlador para contatar o titular, tais como~~,~~ telefone, e-mail, mensagem eletrônica ou carta.

§ 3º Caso a comunicação direta e individualizada se mostre inviável ou não seja possível determinar, parcial ou integralmente, os titulares afetados, o controlador deverá comunicar a ocorrência do incidente, no prazo e com as informações definidas no *caput*, pelos meios de divulgação disponíveis, tais como ~~na sua~~ **seu sítio eletrônico** ~~página na Internet~~, ~~em~~ aplicativos, ~~em~~ suas mídias sociais e ~~em~~ canais de atendimento ao titular, de modo que a comunicação permita o conhecimento amplo, com direta e fácil visualização, pelo período de, no mínimo, ~~seis~~ **três** meses.

§ 4º O controlador deverá juntar ao processo de comunicação do incidente uma declaração de que foi realizada a comunicação aos titulares, constando os meios de comunicação ou divulgação utilizados, em até três dias úteis, contados do término do prazo de que trata o *caput* deste artigo.

§ 5º Em caso de recomendação de autoridade policial ou judiciária para que os titulares não sejam comunicados no prazo de que trata o *caput* deste artigo, por causa de investigação criminal, o controlador deverá juntar ao processo de comunicação do incidente:

I - documento comprobatório emitido pela autoridade policial ou judiciária, com indicação do número do processo ou do procedimento investigatório;

II - a declaração de que trata o § 4º deste artigo em até 3 (três) dias úteis contados do término da recomendação de não comunicação.

§~~4º~~**6º A ANPD poderá determinar ao controlador que comunique o incidente de segurança ao titular quando não o houver comunicado ou a comunicação realizada tenha sido inadequada.** ~~A ANPD determinará que o controlador faça nova comunicação, caso a primeira não contenha todas as informações necessárias ou tenha se utilizado de meios inadequados, ou ainda que comunique o incidente de segurança ao titular, caso a comunicação não tenha sido realizada.~~

§ ~~5º~~**7º** Poderá ser considerada boa prática para fins do disposto no art. 52, § 1º, IX, da LGPD, a inclusão**,** na comunicação ao titular**,** de recomendações aptas a reduzir os efeitos do incidente.

§ ~~6º~~**8º** Os prazos constante**s** no *caput* **e no § 1º** deste artigo conta-se em dobro para os agentes de pequeno porte, nos termos do disposto no Regulamento de aplicação da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) aos agentes de tratamento de pequeno porte, aprovado pela Resolução CD/ANPD nº 2, de 27 de janeiro de 2022.

Regulamento - Cap. IV - Do registro de incidentes de segurança com dados pessoais:

236. A minuta do regulamento colocada em consulta pública tem o seguinte texto para essa seção:

> CAPÍTULO IV
>
> DO REGISTRO DE INCIDENTE DE SEGURANÇA COM DADOS PESSOAIS
>
> Art. 10. O controlador deverá manter o registro de incidentes de segurança com dados pessoais, inclusive daqueles não comunicados à ANPD e aos titulares, pelo prazo mínimo de cinco anos, contados a partir da data do registro, exceto se constatadas obrigações adicionais que demandem maior prazo de manutenção.
>
> § 1º O registro do incidente deve conter, no mínimo:
>
> I - a data de conhecimento do incidente;
>
> II - a descrição geral das circunstâncias em que o incidente ocorreu;
>
> III - a natureza e a categoria de dados afetados;
>
> IV - o número de titulares afetados;
>
> V - a avaliação do risco e os possíveis danos aos titulares;
>
> VI - as medidas de correção e mitigação dos efeitos do incidente, quando aplicável;
>
> VII - a forma e o conteúdo da comunicação, se o incidente foi comunicado à ANPD e aos titulares; e
>
> VIII - os motivos da ausência de comunicação, quando for o caso.
>
> § 2º Os prazos de guarda previstos neste artigo não se aplicam às entidades previstas no art. 23 da LGPD, desde que sejam observadas as regras aplicáveis aos documentos de guarda permanente previstas na tabela de temporalidade própria ou definidas pelo Conselho Nacional de Arquivos.

<u>Contribuições recebidas</u>:

237. Das contribuições apresentadas para este capítulo, destacam-se, pela relevância, as seguintes sugestões:

238. Houve sugestões no sentido de que o operador também tenha a obrigação de manter o registro de incidentes de segurança com dados pessoais; que o encarregado de dados assine, com firma reconhecida em cartório ou por meio de assinatura digital, juntamente com o controlador, o registro de incidente de segurança; que o prazo mínimo de cinco anos disposto no caput do art. 10 seja diminuído, pois um prazo longo implicaria em um maior risco à segurança e à privacidade e poderia contrariar o princípio da minimização; que o registro de incidentes de segurança seja obrigatório apenas para incidentes de segurança significativos (ainda que não comunicáveis), relevantes ou que possam acarretar risco ou dano relevante aos titulares; que o momento de início da contagem do prazo de cinco anos seja modificado, passando de “a partir da data do registro” para “a partir da

data da ciência pelo controlador do incidente de segurança", "a partir da data da ocorrência do incidente de segurança com dados pessoais ou do prazo da cessação da continuidade ou permanência do incidente de segurança"; que o 1º deveria ser complementado com informações do art. 48 da LGPD; que deveria ser incluída conceituação quanto à expressão "registro de incidentes de segurança com dados pessoais"; que deveria ser incluído, no rol do § 1º, a data da confirmação do incidente ou que inciso I do § 1º deveria ser alterado de modo a refletir a data de confirmação do incidente, uma vez que apenas incidentes confirmados devem ser considerados e não incidentes que ensejam apenas suspeitas; que o inciso IV do § 1º seja alterado, para que passe a vigorar com a redação de que o número de titulares afetados deve ser registrado apenas nos casos em que seja possível confirmá-lo; que, no inciso IV do § 1º, o número de titulares possa ser exato ou aproximado ou que a informação seja provida quando "tecnicamente viável"; e que a obrigação de manter registro de incidente de segurança para ATPP seja afastada, tendo em vista que ensejaria custos consideráveis.

239. Além disso, houve dúvida relacionada ao escopo do § 1º, qual seja, se estariam incluídos os próprios dados pessoais comprometidos no incidente, uma vez que o rol trata das informações mínimas a compor o registro de incidentes de segurança.

240. Abaixo serão analisadas as principais contribuições apresentadas para cada um dos dispositivos constantes no art. 10 do regulamento e avaliadas as providências julgadas pertinentes.

Análise:

241. Com relação à atribuição de responsabilidades ao operador relacionadas ao registro de incidentes de segurança com dados pessoais, o art. 50 da LGPD dispõe que controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais. Dessa maneira, controles internos enquadram-se no âmbito da governança do controlador.

242. Em atenção à contribuição para que o encarregado assine, em conjunto com o controlador, os documentos relativos ao registro de incidentes de segurança com dados pessoais, cumpre ressaltar que é competência do controlador comunicar aos titulares, nos termos do art. 48 da LGPD. Caso a ANPD trate da forma de participação do encarregado na notificação de incidente aos titulares, entende-se mais adequado tratar no projeto regulatório que regulamenta a atuação do encarregado.

243. Quanto ao prazo de cinco anos, deve-se observar a Lei nº 9.873, de 23 de novembro de 1999, que, em seu art. 1º, dispõe: "prescreve em cinco anos a ação punitiva da Administração Pública Federal, direta e indireta, no exercício do poder de polícia, objetivando apurar infração à legislação em vigor, contados da data da prática do ato ou, no caso de infração permanente ou continuada, do dia em que tiver cessado". Portanto, o prazo de cinco anos previsto no regulamento será mantido.

244. Quanto às contribuições acerca do registro de incidentes de segurança ser obrigatório apenas para incidentes de segurança significativos (ainda que não comunicáveis), relevantes ou que possam acarretar risco ou dano relevante aos titulares, seu objetivo é manter uma base de informações acerca dos incidentes para que venham subsidiar análises da ANPD em um momento futuro, caso haja necessidade. Portanto, por exemplo, um incidente que venha a ser considerado como não comunicável em um primeiro momento, pode ser avaliado de maneira distinta posteriormente, caso em que a ANPD poderá solicitar os registros. Assim, mesmo incidentes não comunicáveis devem ser objeto do registro em questão.

245. Quanto ao momento de início da contagem do prazo de cinco anos disposto no artigo em questão, não se vislumbra correlação lógica em se considerar o termo inicial do prazo de guarda como, por exemplo, a data da ciência pelo controlador do incidente ou a data da ocorrência do incidente, pois faz necessário consolidar todas as informações necessárias ao registro para que o incidente seja efetivamente registrado. Por consequência lógica, somente se pode contar o prazo de um incidente registrado a partir do momento em que ele foi registrado.

246. Com relação ao escopo do § 1º, se estariam incluídos os próprios dados pessoais comprometidos no incidente, não se vislumbra ambiguidade no parágrafo em questão que possa ensejar interpretação diversa.

247. Em atenção à sugestão de correspondência com o art. 48 da LGPD, destaca-se que tal dispositivo não trata de registro de incidentes de segurança, mas sim da comunicação de incidentes. O registro previsto no artigo do RCIS ora em análise é deveras mais abrangente e distinto, ao incluir até mesmo incidentes não comunicáveis.

248. Quanto à inclusão da conceituação de “registro de incidentes de segurança com dados pessoais”, possivelmente no art. 3º do RCIS, indefere-se a sugestão, tendo em vista que já consta o conceito de incidente de segurança no regulamento, e o registro trata-se de uma atividade do próprio incidente, não ensejando a necessidade de criação de um conceito a ser inserido no art. 3º.

249. Relativo às contribuições que sugeriram a inclusão, no § 1º, da data de confirmação do incidente, constata-se que não há ambiguidade no texto do artigo em questão, ou seja, apenas incidentes confirmados devem ser objeto do registro. Portanto, não se vislumbra necessária a inclusão da

data sugerida.

250. Quanto às sugestões de alteração do inciso IV do § 1º, para que passe a vigorar com a redação de que o número de titulares afetados deve ser registrado apenas nos casos em que seja possível confirmá-lo, que possa ser exato ou aproximado ou que a informação seja provida quando "tecnicamente viável", a CGN entende por não acatar, uma vez que se trata de valor de referência e caso seja inserido o termo aproximado deveria ser definida a metodologia de aproximação. Entende-se afastar o termo tecnicamente viável, tendo em vista que é basilar que o controlador tenha o controle e a organização do banco de dados. Essas medidas são importantes e educacionais, visando uma melhor governança dos dados tratados.

251. Quanto à sugestão de ficar afastada a obrigação de manter registro de incidente de segurança para ATPP, a lei não prevê tal possibilidade, mas apenas que os procedimentos estabelecidos sejam simplificados e diferenciados, motivo pelo qual foi indeferida a contribuição.

Proposta de nova redação para os dispositivos em pauta:

252. Após a análise das contribuições acima citadas, é apresentada a nova proposta redacional, sendo que as redações suprimidas se encontram tachadas e as inseridas em negrito, para melhor compreensão da proposta:

> CAPÍTULO IV
>
> DO REGISTRO ~~DE~~ **DO** INCIDENTE~~S~~ DE SEGURANÇA COM DADOS PESSOAIS
>
> Art. 10. O controlador deverá manter o registro ~~de~~ **do** incidente~~s~~ de segurança com dados pessoais, inclusive daquele~~s~~ não comunicado~~s~~ à ANPD e aos titulares, pelo prazo mínimo de cinco anos, contado~~s~~ a partir da data do registro, exceto se constatadas obrigações adicionais que demandem maior prazo de manutenção.
>
> § 1º O registro do incidente deve**rá** conter, no mínimo:
>
> I - a data de conhecimento do incidente;
>
> II - a descrição geral das circunstâncias em que o incidente ocorreu;
>
> III - a natureza e a categoria de dados afetados;
>
> IV - o número de titulares afetados;
>
> V - a avaliação do risco e os possíveis danos aos titulares;
>
> VI - as medidas de correção e mitigação dos efeitos do incidente, quando aplicável;
>
> VII - a forma e o conteúdo da comunicação, se o incidente ~~foi~~ **tiver sido** comunicado à ANPD e aos titulares; e
>
> VIII - os motivos da ausência de comunicação, quando for o caso.
>
> § 2º Os prazos de guarda previstos neste artigo não se aplicam às entidades previstas no art. 23 da LGPD, desde que sejam observadas

as regras aplicáveis aos documentos de guarda permanente previstas na tabela de temporalidade própria ou definidas pelo Conselho Nacional de Arquivos.

Regulamento - Cap. V - Seção I - Das disposições gerais:

253. A minuta do regulamento colocada em consulta pública tem o seguinte texto para essa seção:

> CAPÍTULO V
>
> DO PROCESSO DE COMUNICAÇÃO DE INCIDENTE DE SEGURANÇA COM DADOS PESSOAIS
>
> Seção I
>
> Das disposições gerais
>
> Art. 11. Aplicam-se ao processo de comunicação de incidente de segurança com dados pessoais regido por este Regulamento as disposições das Seções I, II e IV do Capítulo IV do Título I do Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador, aprovado pela Resolução CD/ANPD nº 01, de 28 de outubro de 2021.
>
> Art. 12. O processo de comunicação de incidente de segurança com dados pessoais pode incluir os seguintes procedimentos:
>
> I - Procedimento de Apuração de Incidente de Segurança; e
>
> II - Procedimento de Comunicação de Incidente de Segurança.
>
> Parágrafo único. O procedimento de apuração de incidente de segurança não é de realização obrigatória, somente sendo iniciado nas hipóteses em que a ANPD tomar conhecimento de um incidente de segurança envolvendo dados pessoais que não tenha sido comunicado pelo controlador nos prazos e nas condições estabelecidas neste Regulamento.
>
> Art. 13. Os processos de comunicação de incidente de segurança com dados pessoais, de que trata este Regulamento, poderão ser analisados de forma agregada, e as eventuais providências deles decorrentes poderão ser adotadas de forma padronizada.
>
> Parágrafo único. Os processos referidos no *caput* serão analisados e, se for o caso, extintos, em conformidade com o planejamento da atividade de fiscalização e os critérios de priorização definidos no Relatório de Ciclo de Monitoramento de que trata o art. 20 do Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador no âmbito da Autoridade Nacional de Proteção de Dados, aprovado pela Resolução nº 1, de 28 de outubro de 2021.
>
> Art. 14. Em qualquer fase do processo de comunicação de incidente de segurança com dados pessoais, a ANPD poderá determinar ao controlador a adoção imediata de medidas preventivas necessárias para salvaguardar direitos dos titulares ou para reverter ou mitigar os efeitos do incidente, sem prévia manifestação do controlador.
>
> Parágrafo único. As medidas referidas no *caput* devem estar

diretamente relacionadas ao incidente de segurança e à salvaguarda dos direitos dos titulares.

Contribuições recebidas:

254. Das contribuições apresentadas para a presente seção da minuta do Regulamento, destacam-se, pela relevância, as seguintes sugestões:

255. Quanto ao art. 11, houve sugestão no sentido de se substituir a expressão "processo de comunicação de incidente de segurança com dados pessoais" por "processo de averiguação de incidente de segurança com dados pessoais", de forma a evitar confusões de entendimento, uma vez que há o "procedimento de comunicação de incidente de segurança com dados pessoais". Tal contribuição permeia outros artigos ao longo do regulamento.

256. Houve também sugestões no sentido de que o processo de comunicação de incidente de segurança deva refletir os princípios da legalidade, ampla defesa e contraditório.

257. Houve, ainda, solicitações de esclarecimentos e inserção de texto acerca da natureza do processo de comunicação de incidente de segurança, se seria uma avaliação sumária do incidente ou se trataria de uma atividade fiscalizatória. Em se tratando do segundo caso, foi solicitado observância ao devido processo legal, através da menção expressa às Resoluções CD/ANPD nº 01/2021 e 04/2023".

258. Por fim, houve sugestão afirmando que a falta de previsão recursal no art. 11 "conduz a questão à aplicação subsidiária da Lei n. 9.784/99".

259. Quanto ao art. 12 do regulamento, houve contribuição no sentido de se substituir a expressão "processo de comunicação de incidente de segurança com dados pessoais" por "processo de averiguação de incidente de segurança com dados pessoais", de forma a evitar confusões de entendimento, uma vez que há o "procedimento de comunicação de incidente de segurança com dados pessoais". Tal contribuição permeia outros artigos ao longo do regulamento.

260. Houve, também, contribuições indicando ambiguidade com relação ao texto do art. 12, sendo que o caput faculta a realização do procedimento de apuração e/ou de comunicação, sendo que apenas o primeiro seria de observância não obrigatória pelo parágrafo único, o que poderia ensejar o entendimento que o inciso II seria obrigatório.

261. Quanto ao art. 13 do regulamento, com relação à análise agregada de incidentes de segurança com dados pessoais, houve contribuições ensejando que seja adicionada ao regulamento a previsão da avaliação individualizada de cada um dos agentes de tratamento envolvidos, devido às particularidades de cada caso concreto, incluindo a fundamentação

individualizada.

262. Nesse sentido, houve contribuição no sentido de se incluir parágrafo ao art. 12, o qual deverá prever que a ANPD deverá justificar todas as decisões por uma análise agregada, indicando os elementos comuns que ensejaram a situação.

263. Outrossim, houve sugestão da previsão de observância aos segredos comercial e industrial no parágrafo único do art. 13.

264. Em relação ao art. 14, houve sugestão para incluir previsão de que a ANPD poderá determinar ao controlador a adoção imediata de medidas preventivas necessárias para salvaguardar direitos dos titulares ou para reverter ou mitigar os efeitos do incidente em qualquer fase do processo de comunicação de incidente de segurança com dados pessoais, após a avaliação da gravidade do incidente.

265. Houve, igualmente, sugestões para que se preveja o contraditório, ampla defesa e devido processo legal nos dispositivos em comento; para que se modifique o termo "imediata", solicitando que a determinação ao controlador de adoção de medidas preventivas seja realizada pontualmente ou que seja indicado um prazo máximo, ou, ainda, para que esse termo seja excluído, pois se trata de um termo abstrato; para que o controlador seja ouvido previamente quanto à viabilidade da implementação das medidas a serem impostas pela ANPD; que a ANPD proceda à publicação de orientação sobre as medidas preventivas cabíveis.

266. Por fim, houve contribuição solicitando que seja fundamentada a determinação emanada pela ANPD, presente no caput do referido artigo, além de sugestão sobre a possibilidade de o controlador "requerer efeito suspensivo à determinação da ANPD dado que o controlador está sujeito - em caso de descumprimento – a (sic) progressão da atuação da ANPD ao modo repressivo (art. 32, § 2º, I, Regulamento do Processo de Fiscalização e Processo Administrativo Sancionador), a ter tal descumprimento considerado como circunstância agravante em caso de instauração de processo administrativo sancionador (art. 32, § 2º, I, do mesmo Regulamento e art. 12, III do Regulamento de Dosimetria e Aplicação de Sanções Administrativas) e à aplicação de multa simples (art.10, I, do Regulamento de Dosimetria e Aplicação de Sanções Administrativas)".

Análise:

267. Em relação ao art. 11, quanto às contribuições que solicitaram a alteração da expressão "processo de comunicação de incidente de segurança com dados pessoais" por "processo de averiguação de incidente de segurança com dados pessoais", embora exista similaridade quanto à redação, o processo de comunicação de incidentes de segurança, objeto da presente análise, é diferenciado do procedimento de comunicação de incidentes de segurança pelo próprio RCIS, em seu art. 12. Portanto, é

possível depreender da leitura que se trata de dispositivos diversos.

268. Em atenção à contribuição sobre obediência aos princípios da legalidade, ampla defesa e contraditório no âmbito do processo de comunicação de incidente de segurança com dados pessoais, cumpre lembrar que não se trata de atividade sancionatória, isto é, de aplicação de penalidade, mas fiscalizatória, sem acusação, a fim de se verificar o cumprimento de obrigações legais e regulatórias. Na atividade de fiscalização, cumpre observar, naturalmente, o devido processo legal.

269. Com relação à contribuição sobre previsão recursal, cabe esclarecer que, nos termos do art. 56 da Lei nº 9.784, de 29 de janeiro de 1999, das decisões administrativas cabe recurso, em face de razões de legalidade e de mérito. O disposto no caput do art. 11 trata da aplicação de dispositivos relacionados a disposições processuais como contagem de prazos, comunicação de atos e atendimento prioritários. Assim, não resta claro a necessidade de previsão quanto a recursos no âmbito do processo de comunicação de incidente de segurança, pois não se trata de processo administrativo sancionador.

270. Em tempo, registra-se que algumas contribuições manifestaram dúvidas sobre a natureza do processo de comunicação de incidentes com dados pessoais. Por esse motivo, a CGN optou por dar nova redação ao caput do dispositivo e transformar o texto do caput em parágrafo único. Veja-se:

> Art. 11. **O processo de comunicação de incidente de segurança com dados pessoais tem por objeto a fiscalização de atos relacionados ao tratamento e resposta ao incidente que possa acarretar risco ou dano relevante aos titulares de dados, a fim de salvaguardar os direitos dos titulares.**
>
> ~~Art. 11~~Parágrafo único. Aplicam-se ao processo de comunicação de incidente de segurança com dados pessoais regido por este Regulamento as disposições das Seções I, II e IV do Capítulo IV do Título I do Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador, aprovado pela Resolução CD/ANPD nº 01, de 28 de outubro de 2021.

271. Quanto ao art. 12, relativamente às contribuições que solicitaram a alteração da expressão “processo de comunicação de incidente de segurança com dados pessoais” por “processo de averiguação de incidente de segurança com dados pessoais”, embora exista similaridade quanto à redação, o processo de comunicação de incidentes de segurança, objeto da presente análise, é diferenciado do procedimento de comunicação de incidentes de segurança pelo próprio Regulamento, em seu art. 12. Enquanto processo é gênero, procedimento é espécie. Portanto, é não há ambiguidade no uso dos termos que necessite ser evitada.

272. Com relação à ambiguidade no texto do art. 12, quanto a possibilidade de facultar a realização do procedimento de apuração e/ou de comunicação, a fim de dirimi-la, procedeu-se a ajustes para evitá-la. Além

disso, exclui-se o parágrafo único, considerando que o art. 3º da minuta do regulamento já prevê a definição de ambos os procedimentos. Veja-se:

> Art. 12. O processo de comunicação de incidente de segurança com dados pessoais inicia-se com ~~pode incluir os seguintes procedimentos~~:
>
> I - ~~P~~**p**rocedimento de ~~A~~**a**puração de ~~i~~**I**ncidente de ~~S~~**s**egurança; ~~e~~ **ou**
>
> II - ~~P~~**p**rocedimento de ~~C~~**c**omunicação de ~~i~~**I**ncidente de ~~S~~**s**egurança.
>
> ~~Parágrafo único. O procedimento de apuração de incidente de segurança não é de realização obrigatória, somente sendo iniciado nas hipóteses em que a ANPD tomar conhecimento de um incidente de segurança envolvendo dados pessoais que não tenha sido comunicado pelo controlador nos prazos e nas condições estabelecidas neste Regulamento.~~

273. Com relação ao art. 13, em atenção à avaliação e fundamentação individualizada de cada agente de tratamento, observadas as particularidades de cada caso concreto, entende-se que, apesar das análises serem agregadas, toda e qualquer avaliação do incidente pela ANPD levará em conta a responsabilização individualizada.

274. Quanto à sugestão de justificativa acerca das decisões por análises agregadas, todos os atos da administração pública devem ser motivados, portanto, a sugestão não se mostra necessária.

275. Quanto aos segredos comercial e industrial, o art. 7º da minuta do Regulamento já prevê que cabe ao controlador solicitar à ANPD, de maneira fundamentada, o sigilo de informações protegidas por lei, indicando aquelas cujo acesso deverá ser restringido, a exemplo das relativas à sua atividade empresarial cuja divulgação possa representar violação de segredo comercial ou industrial.

276. Sobre o art. 14, preliminarmente, convém esclarecer que se trata de dispositivo inspirado no inciso II do § 2º do art. 48 da LGPD e fundamentado no art. 45 da Lei nº 9.784, de 1999 (Lei de Processo Administrativo). Com isso, esse dispositivo busca prever o exercício do poder geral de cautela pela Autoridade, conforme item 91 do Parecer 00023/2022/GAB/PFE/ANPD/PGF/AGU (3819738), ao explicar que as medidas de polícia administrativa previstas no inciso II do §2º têm a natureza acautelatória, acrescentando que essas determinações devem ser sempre proporcionais à finalidade indicada. O dispositivo objetiva possibilitar que a Coordenação-Geral de Fiscalização determine, cautelarmente, ao controlador, a adoção de providências ou medidas, caso necessário para a salvaguarda dos direitos dos titulares. Considerando que as providências serão exclusivamente baseadas nos casos concretos, a depender da gravidade do incidente, e a ANPD ainda está ganhando maturidade quanto ao contexto do ambiente regulado, parece ser prudente não especificar de modo exaustivo as medidas que poderiam ser determinadas. No entanto, quanto ao ponto sobre a possibilidade de se pedir concessão de efeito suspensivo dessa medida, entende-se pela necessidade de prever dispositivo quanto a prazo

recursal para a decisão que determinar a medida, com menção a efeito suspensivo.

277. Em relação a esse poder geral de cautela de que trata o art. 48, § 2º, II, da LGPD, a competência correspondente consta inscrita no Decreto nº 10.474, de 2020, e na Portaria nº 1, de 2021 (Regimento Interno da ANPD). Nos termos do art. 4º, V, "b", do Decreto nº 10.474, de 2021, compete ao Conselho Diretor determinar a adoção de providências para a salvaguarda dos direitos dos titulares, a partir da verificação da gravidade de incidentes de segurança. Já nos termos do art. 17, XXII, do RIANPD, compete à CGF determinar ao controlador de dados pessoais a adoção de providências para a salvaguarda dos direitos dos titulares, a partir da verificação da gravidade de incidentes de segurança, sem prejuízo da aplicação de correspondente sanção.

278. Nesse sentido, ainda no âmbito do RIANPD, verifica-se que, nos termos de seu art. 55, consta a possibilidade quando se tratar do exercício do poder geral de cautela pelo Conselho Diretor da ANPD. Veja-se:

> Art. 55. **Os Diretores do Conselho Diretor da ANPD poderão, motivadamente e observadas as competências estabelecidas neste Regimento, adotar medidas preventivas** indispensáveis para evitar dano grave e irreparável ou de difícil reparação, de ofício ou mediante a prévia manifestação dos interessados.
>
> § 1º Até que eventual pedido de concessão de efeito suspensivo seja julgado, todas as decisões previstas na medida preventiva deverão ser cumpridas.
>
> § 2º A decisão do pedido de concessão de efeito suspensivo terá caráter urgente e prioritário em face dos demais.
>
> § 3º As medidas preventivas podem ser adotadas no curso do procedimento ou, em caso de risco iminente, antes dele.
>
> § 4º Assim que possível, o processo no qual tenha sido proferida medida preventiva deverá ser encaminhado para deliberação do Conselho Diretor.

279. Além disso, nos termos do inciso IV do art. 26 do Anexo I do Decreto nº 10.474, de 26 de agosto de 2020, e do inciso IV do art. 7º do RIANPD, *adotar medidas preventivas e fixar o valor da multa diária pelo seu descumprimento, no âmbito de processos de sua relatoria* é atribuição dos Diretores. Quanto à CGF, a esta cabe *propor a adoção de medidas preventivas e fixar o valor da multa diária pelo seu descumprimento*, nos termos do inciso V do art. 17 do RIANPD.

280. Desse modo, conforme item 123 do Parecer 00023/2022/GAB/PFE/ANPD/PGF/AGU (3819738), há uma convivência da redação proposta no art. 14 da minuta, que era numerado como art. 27 quando da avaliação pela PFE, com outros dispositivos que têm natureza cautelar, previstos no âmbito da ANPD, tendo em vista a especificidade da medida inscrita no art. 14 da minuta em relação às medidas preventivas de caráter geral previstas no art. 26 do Decreto nº 10.474, de 2020,

e espelhadas nos artigos 7º, IV, e 55 do Regimento Interno da ANPD, relacionados ao art. 45 da Lei nº 9.784, de 1999.

281. No caso do art. 14 da minuta, a ideia é que a autoridade competente para decidir sobre a determinação de adoção de medida acautelatória ou assecuratória de caráter mais específico seja a CGF. Assim, caberá, então, recurso ao Conselho Diretor. Por esse motivo, sugere-se alterar a redação do parágrafo único, passando a constar o prazo para recurso da decisão, com possibilidade de efeito suspensivo, na esteira do art. 55 do RIANPD. Ainda nesta esteira, sugere-se incluir também a possibilidade de haver oitiva do interessado, caso a CGF entenda que o caso concreto possibilite esse manejo frente ao risco iminente envolvido, uma vez que o controlador poderá, ao apresentar suas justificativas, esclarecer eventuais mal-entendidos interpretativos por parte desta Autoridade.

282. Dessarte, torna-se oportuno propor nova redação ao art. 14, de modo a torná-lo mais claro e conciso, a possibilitar determinações com ou sem a manifestação do controlador, a depender do caso concreto, e indicar prazo para recurso da decisão – de 10 (dez) dias úteis, de modo análogo ao art. 58 da Resolução CD/ANPD nº 1, de 28 de outubro de 2021 –, com pedido de concessão de efeito suspensivo, em redação inspirada no art. 55 do RIANPD:

> Art. 14. ~~Em qualquer fase do processo de comunicação de incidente de segurança com dados pessoais, a ANPD poderá determinar ao controlador a adoção imediata de medidas preventivas necessárias para salvaguardar direitos dos titulares ou para reverter ou mitigar os efeitos do incidente, sem prévia manifestação do controlador.~~ **No curso do processo de comunicação de incidente de segurança com dados pessoais, em caso de risco iminente, a ANPD poderá determinar ao controlador, após avaliar a gravidade do incidente, a adoção imediata de medidas necessárias para salvaguardar direitos dos titulares, a fim de prevenir, mitigar ou reverter os efeitos do incidente, com ou sem prévia manifestação do controlador.**
>
> ~~Parágrafo único.~~ **§ 1º** ~~As medidas referidas no *caput* devem estar diretamente relacionadas ao incidente de segurança e à salvaguarda dos direitos dos titulares~~. **Da decisão de determinação da medida caberá recurso, no prazo de 10 (dez) dias úteis, ao Conselho Diretor.**
>
> **§ 2º Até que eventual pedido de concessão de efeito suspensivo seja julgado, todas as medidas previstas na decisão deverão ser cumpridas.**

<u>Proposta de nova redação para os dispositivos em pauta:</u>

283. Preliminarmente, registra-se que a CGN entendeu pela exclusão da expressão “de que trata este Regulamento” no caput do art. 13, ao referir-se ao processo de comunicação de incidente de segurança com dados pessoais, em razão da redundância por ela provocada.

284. Com isso, após a análise das contribuições acima citadas, é apresentada a nova proposta redacional, sendo que as redações suprimidas

se encontram tachadas e as inseridas em negrito, para melhor compreensão da proposta:

CAPÍTULO V

DO PROCESSO DE COMUNICAÇÃO DE INCIDENTE DE SEGURANÇA COM DADOS PESSOAIS

Seção I

Das disposições gerais

Art. 11. O processo de comunicação de incidente de segurança com dados pessoais tem por objeto a fiscalização de atos relacionados ao tratamento e resposta ao incidente que possa acarretar risco ou dano relevante aos titulares de dados, a fim de salvaguardar os direitos dos titulares.

~~Art. 11.~~ **Parágrafo único.** Aplicam-se ao processo de comunicação de incidente de segurança com dados pessoais regido por este Regulamento as disposições das Seções I, II e IV do Capítulo IV do Título I do Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador, aprovado pela Resolução CD/ANPD nº 01, de 28 de outubro de 2021.

Art. 12. O processo de comunicação de incidente de segurança com dados pessoais **inicia-se com** ~~pode incluir os seguintes procedimentos~~:

I - ~~P~~**p**rocedimento de ~~A~~**a**puração de ~~i~~**I**ncidente de ~~S~~**s**egurança; ~~e~~ **ou**

II - ~~P~~**p**rocedimento de ~~C~~**c**omunicação de ~~i~~**I**ncidente de ~~S~~**s**egurança.

~~Parágrafo único. O procedimento de apuração de incidente de segurança não é de realização obrigatória, somente sendo iniciado nas hipóteses em que a ANPD tomar conhecimento de um incidente de segurança envolvendo dados pessoais que não tenha sido comunicado pelo controlador nos prazos e nas condições estabelecidas neste Regulamento.~~

Art. 13. Os processos de comunicação de incidente de segurança com dados pessoais~~, de que trata este Regulamento,~~ poderão ser analisados de forma agregada, e as eventuais providências deles decorrentes poderão ser adotadas de forma padronizada.

Parágrafo único. Os processos referidos no *caput* serão analisados e, se for o caso, extintos, em conformidade com o planejamento da atividade de fiscalização e os critérios de priorização definidos no Relatório de Ciclo de Monitoramento de que trata o art. 20 do Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador no âmbito da Autoridade Nacional de Proteção de Dados, aprovado pela Resolução **CD/ANPD** nº 1, de 28 de outubro de 2021.

Art. 14. ~~Em qualquer fase do processo de comunicação de incidente de segurança com dados pessoais, a ANPD poderá determinar ao controlador a adoção imediata de medidas preventivas necessárias para salvaguardar direitos dos titulares ou para reverter ou mitigar os efeitos do incidente, sem prévia manifestação do controlador.~~ **No curso do processo de comunicação de incidente de segurança com**

dados pessoais, em caso de risco iminente, a ANPD poderá determinar ao controlador, após avaliar a gravidade do incidente, a adoção imediata de medidas necessárias para salvaguardar direitos dos titulares, a fim de prevenir, mitigar ou reverter os efeitos do incidente, ou sem prévia manifestação do controlador.

~~Parágrafo único.~~ **§ 1º** ~~As medidas referidas no *caput* devem estar diretamente relacionadas ao incidente de segurança e à salvaguarda dos direitos dos titulares~~. **Da decisão caberá recurso, no prazo de 10 (dez) dias úteis, ao Conselho Diretor.**

§ 2º Até que eventual pedido de concessão de efeito suspensivo seja julgado, todas as medidas previstas na decisão deverão ser cumpridas.

Regulamento - Cap. V - Seção II - Do procedimento de apuração de incidente de segurança:

285. A minuta do regulamento colocada em consulta pública tem o seguinte texto para essa seção:

> Seção II
>
> Do procedimento de apuração de incidente de segurança
>
> Art. 15. A ANPD poderá apurar, por meio do procedimento de apuração de incidente, a ocorrência de incidentes de segurança com dados pessoais que possam acarretar risco ou dano relevante aos titulares não comunicados pelo controlador de que venha a tomar conhecimento.
>
> § 1º A ANPD poderá requisitar ao controlador informações para apurar a ocorrência do incidente de segurança.
>
> § 2º A ANPD avaliará a ocorrência do incidente que possa acarretar risco ou dano relevante aos titulares por meio dos critérios dispostos no art. 5º deste Regulamento.
>
> Art. 16. A ANPD determinará ao controlador o envio da comunicação do incidente à Autoridade e aos titulares, quando identificar a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares de dados que não tenha sido comunicado pelo controlador.
>
> § 1º A ANPD poderá fixar multa diária para assegurar o cumprimento da determinação prevista no *caput*.
>
> § 2º A ANPD poderá, ainda, instaurar processo administrativo sancionador para apurar o descumprimento do previsto nos arts. 6º e 9º deste Regulamento.

286. Das contribuições apresentadas para esta seção, destacam-se, pela relevância, as seguintes sugestões:

287. Quanto ao art. 15, houve contribuições no sentido de se prever o contraditório, a ampla defesa e o devido processo legal; acerca da definição de prazo para que o controlador atenda às solicitações da ANPD, tendo como

sugestão 20 (vinte) dias ou "prazo razoável"; de se incluir texto para que a abertura do procedimento de apuração seja justificada pela ANPD; e para que sejam previstos os segredos comercial e industrial.

288. Em relação ao art. 16, houve contribuições a fim de que a multa prevista no § 1º seja fixada após a notificação do controlador e este deixar de sanar as irregularidades no prazo fixado; se explicite a contagem do prazo em conformidade com os artigos 6º e 9º, já que o controlador seria cientificado por meio da notificação da ANPD, para incrementar a segurança jurídica da disposição; se preveja o contraditório, ampla defesa e devido processo legal; se defina o prazo para que o controlador atenda às solicitações da ANPD, sugerindo-se 20 dias (vinte) úteis ou 5 (cinco) dias úteis, no mínimo).

289. Houve, ainda, contribuição no sentido de que a previsão de multa pode resultar em um duplo sancionamento, vez que poderá ser aberto processo sancionador conforme Resolução nº 1 CD/ANPD. Com isso, sugeriu-se incluir "determinar que a não comunicação de incidente será apurada e sancionada nos termos das Resoluções n. 1 e 4 da ANPD". No mesmo sentido, outras contribuições solicitaram que a multa deve ser posterior à instauração de um processo administrativo sancionador. E, ainda, afirmaram que o texto suscita dúvidas se a multa faria parte do processo de apuração do incidente ou de um processo sancionador. Nessa esteira, houve contribuição a fim de prever fixação de teto para valor acumulado da multa, mencionando-se o art. 52, II, da LGPD, e Resolução CD/ANPD nº 4, de 24 de fevereiro de 2023.

Análise:

290. Em referência às contribuições para o art. 15, com relação às sugestões de inserção no texto do regulamento sobre a previsão do contraditório, ampla defesa e devido processo legal, registra-se que o procedimento de apuração tem natureza investigativa, inquisitorial, não havendo se falar em ampla defesa e contraditório nesse momento. Em atenção à definição de um prazo para que o controlador atenda às solicitações da ANPD, esse dependerá do caso concreto. Quanto à inclusão textual para que a abertura do procedimento de apuração seja justificada pela ANPD, ressalta-se que todos os atos da administração pública devem ser motivados. Quanto aos segredos comercial e industrial, o tema já foi bem tratado em seções anteriores desta Nota, além de que o art. 7º da minuta já prevê que cabe ao controlador solicitar à ANPD, de maneira fundamentada, o sigilo de informações protegidas por lei, indicando aquelas cujo acesso deverá ser restringido, a exemplo das relativas à sua atividade empresarial cuja divulgação possa representar violação de segredo comercial ou industrial.

291. Em relação às contribuições ao art. 16, registra-se, inicialmente, que, a partir de um procedimento de apuração, pode-se constatar ou que controlador avaliou adequadamente que o incidente não se enquadrava como comunicável, nos termos do art. 5º da minuta do Regulamento, ou que

houve descumprimento da obrigação imposta pelo art. 48 da LGPD, quer por avaliação inadequada, quer por ato volitivo. Ainda, cumpre esclarecer que esse dispositivo foi incluído na minuta do Regulamento em razão do Voto nº 8/2023/DIR/JR/ANPD (4171788). Segue sua motivação:

> h. Da fixação da multa diária
>
> Na esteira da modificação anteriormente exposta, julgo conveniente indicar de forma expressa a possibilidade de fixação de multa diária em caso de não cumprimento da determinação de apresentação de comunicação potencialmente realizada ao final do procedimento de apuração de incidente de segurança.
>
> Como indicado, este procedimento, que será autônomo em relação ao procedimento de comunicação de incidentes, se presta à apuração pela ANPD quanto a incidentes não comunicados pelos controladores nas condições estabelecidas pelo normativo. Desta forma, quando identificado um incidente envolvendo dados pessoais capaz de gerar risco ou dano relevante aos titulares, a equipe da CGF determinará ao controlador que apresente a comunicação, como forma de viabilizar a apuração aprofundada do incidente e, se for o caso, poderá determinar a adoção de providencias para a salvaguarda dos direitos e interesses dos titulares afetados.
>
> Assim, nota-se que a apresentação da comunicação do incidente pelo controlador representa condição para o prosseguimento da atuação da ANPD, sem a qual não seria possível o conhecimento completo pela equipe da fiscalização sobre o incidente e seus eventuais desdobramentos, inviabilizando, ainda, a avaliação quanto à necessidade de adoção de medidas para a mitigação ou reversão dos impactos decorrentes do incidente.
>
> Desta forma, com o objetivo de direcionar o comportamento dos agentes de tratamento e, ainda, garantir mais efetividade à atuação da autoridade, desestimulando a eventual inércia por parte dos controladores, alterei a redação do atual artigo 16 da minuta, inserindo parágrafo a prever especificamente a possibilidade de fixação de multa diária em caso de descumprimento da determinação da ANPD de envio da comunicação do incidente.

292. Verifica-se, então, que o propósito do parágrafo incluído tem por objetivo direcionar o comportamento dos agentes de tratamento e, ainda, garantir mais efetividade à atuação da autoridade, desestimulando a eventual inércia por parte dos controladores, quando da determinação da CGF para que o controlador apresente a comunicação sobre o incidente à ANPD e aos titulares.

293. Diante da motivação esposada, depreende-se que se trata da possibilidade de fixação de multa cominatória (astreintes), na qualidade não de sanção administrativa, mas de medida de polícia administrativa, a fim de inibir o descumprimento de determinação emanada de decisão da CGF que vise a comunicação do incidente à ANPD e ao titular de dados.

294. O poder de polícia no âmbito do Direito Administrativo, em termos simples, trata-se de um poder estatal não jurisdicional concretizado a partir da edição de atos administrativos normativos, expressando uma

obrigação de fazer ou não fazer e que tem como fundamento mais do que a mera supremacia do interesse público sobre o privado, mas a defesa dos direitos fundamentais. No microssistema de proteção de dados pessoais, é possível verificar que, enquanto direito e tendo na ANPD o seu maior guardião, esta Autoridade possui o poder de polícia no fundamental contexto da proteção de dados pessoais para garantir o cumprimento das normas da Lei Geral de Proteção de Dados (LGPD). Esse poder de polícia é fundamental para assegurar os direitos dos titulares de dados e para garantir a conformidade dos agentes de tratamento de dados com as disposições da LGPD. A LGPD estabelece regras rígidas para a proteção dos dados pessoais, e a ANPD é a autoridade responsável por supervisionar e fiscalizar o cumprimento dessas regras.

295. No contexto do regulamento de comunicados de incidentes de segurança com dados pessoais, no seu art. 16, a ANPD exerce seu poder de polícia para compelir os agentes de tratamento de dados a cumprir com suas obrigações regulamentares, a partir de uma prescrição mandamental inscrita na própria LGPD. Assim, quando um agente de tratamento toma conhecimento de um incidente de segurança com dados pessoais que pode ocasionar risco ou dano relevante, ele tem a obrigação de comunicar o incidente à ANPD e aos titulares de dados afetados, conforme o artigo 48 da LGPD.

296. No entanto, em situações em que o agente de tratamento está ciente de um incidente com possibilidade de risco ou dano relevante ao titular, mas não o comunica à Autoridade e ao titular dos dados, a ANPD pode impor medidas acautelatórias como parte de seu poder de polícia. Nesse caso, a ANPD poderá aplicar uma multa diária de caráter cominatório e não sancionatório com o objetivo de compelir o agente de tratamento a comunicar o incidente o mais rápido possível dados riscos em que o titular de dados pode estar exposto, dependendo do caso concreto.

297. A imposição de uma multa diária cominatória é uma medida eficaz para garantir a conformidade do agente de tratamento com a obrigação de comunicação e a proteção dos direitos dos titulares de dados, uma vez que cria um incentivo financeiro para que os agentes de tratamento cumpram suas obrigações legais sem demora. Ressalte-se que, em que pese a previsão de multa diária no artigo 52 da LGPD, de natureza sancionatória, na presente minuta tal multa possui natureza diversa, funcionando como medida que visa garantir o cumprimento das obrigações legais estabelecidas na LGPD, ainda no âmbito de processo administrativo fiscalizatório e, mais especificamente, no procedimento de apuração previsto na proposta de Regulamento.

298. Mais especificamente, interessa esclarecer aqui, portanto, a natureza jurídica dessa multa diária e, ainda, a possibilidade de sua imputação sem a expressa autorização legal. Isso porque as atividades administrativas devem ser regidas, primordialmente, pelo princípio da legalidade, em outras palavras, a administração pública só pode fazer aquilo

que a lei autoriza expressamente, ou seja, a administração só pode agir com base na lei. Isto significa que a administração pública não possui poderes discricionários ilimitados, e suas ações devem estar estritamente de acordo com a legislação vigente. Tal princípio garante que o administrador atue de forma previsível e transparente frente à sociedade, administrados e, por conseguinte, regulados.

299. No caso específico da multa diária prevista no art. 16 da minuta em comento, tem-se que, apesar da sua não expressa previsão na LGPD, existe a previsão normativa do poder geral de cautela do art. 45 da Lei nº 9784/1999, possibilitando a adoção de medidas provisionais atípicas, ou seja, não previstas expressamente em lei. No entanto, é importante destacar que a falta de tipicidade na adoção de medidas cautelares não implica em uma autorização indiscriminada para a implementação de qualquer tipo de providência. As medidas cautelares fundamentadas no artigo 45 da Lei 9.789/1999 devem estar diretamente relacionadas com o objetivo desejado, com a devida motivação, respeitados o princípio da proporcionalidade, além do contraditório e da ampla defesa, mesmo que em momento ulterior e em sede de recurso.

300. Ademais, não se pode considerar que, no caso da regulamentação em análise, uma vez não comunicado o incidente no prazo previsto e aberto o procedimento de apuração, a mera determinação pela ANPD ao controlador de comunicar o incidente será suficiente. Com efeito, no trabalho fiscalizatório da Autoridade, especificamente no caso dos comunicados, as obrigações de fazer devem ser acompanhadas de medidas coercitivas concretas, fruto de decisão objetivamente motivada, a fim de que possam ser cumpridas e respeitadas.

301. Resta saber, nesse contexto, se há suporte legal para a fixação da multa diária como medida coercitiva por parte da ANPD no âmbito do processo de comunicação do incidente. A resposta parece afirmativa quando se observa o §2º do art. 48:

> §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.

302. É importante salientar, nesse aspecto, que o rol de providências é exemplificativo, cabendo à ANPD definir outras determinações com fins de salvaguarda dos direitos dos titulares. Nesse mesmo esteio, tem-se o art. 55-J, prescrevendo a competência da Autoridade em fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso, mesmo que ulterior à medida, frise-se. Por fim, tem-se o comando insculpido no Decreto nº 10.474/2020, art. 26, IV, que prevê a competência dos Diretores do Conselho Diretor de adotar medidas preventivas e fixar o valor da multa diária pelo seu

descumprimento, competência esta reproduzida no Regimento Interno da ANPD, no art. 7º, IV.

303. Nesse ponto, nos termos do art. 17, V do RIAP da ANPD, cabe à Coordenação-Geral de Fiscalização propor ao Conselho Diretor a adoção de medidas preventivas, inclusive a fixação do valor da multa diária pelo seu descumprimento, enquanto que ao Conselho Diretor caberá fixar o valor de tal multa.

304. Assim, não faz sentido admitir que a Autoridade, na sua missão precípua de proteger os dados pessoais dos titulares e no exercício do seu poder geral de cautela, possa determinar providências sem que para isso detenha as ferramentas - *id est*, multa diária - que devem ser utilizadas como meio coercitivo de cumprimento dessa mesma determinação.

305. Nesse sentido, é possível afirmar que, havendo previsão legal (mesmo que genérica, como é o caso do art. 45 da LPA), a multa diária de caráter não sancionatório, mas de medida coercitiva de polícia, prevista no art. 16, pode ser utilizada para garantir o cumprimento de uma ordem ou determinação que contenha uma obrigação de fazer ou não fazer. No caso em análise, a ANPD poderá compelir o agente de tratamento a comunicar o incidente de segurança com dados pessoais aos titulares, sob pena de imputação de uma multa diária, desde que realizada por autoridade competente e devidamente justificada (motivação do ato administrativo).

306. Por fim, propõe-se nova redação ao art. 16, de modo a torná-lo mais completo, indicando o prazo e condições para cumprimento da determinação, bem como prazo para recurso da decisão – de 3 (três) dias úteis, o mesmo prazo para cumprimento da medida, pois, se superior, a medida irreversível prejudica o recurso –, com efeito suspensivo, porque, como dito alhures, em um procedimento de apuração, pode-se constatar ou que controlador avaliou adequadamente que o incidente não se enquadrava como comunicável nos termos do art. 5º da minuta do Regulamento ou que houve descumprimento da obrigação imposta pelo art. 48 da LGPD, quer por avaliação inadequada, quer por ato deliberado.

307. Nesse esteio, tendo em vista a competência do Conselho Diretor para fixar multa diária, não havendo instância administrativa superior para interposição de recurso e, a fim de preservar os princípios do contraditório e ampla defesa, caberá pedido de reconsideração sobre a decisão. Veja-se:

> Art. 16. A ANPD determinará ao controlador o envio da comunicação do incidente à Autoridade e aos titulares, quando identificar a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares de dados que não tenha sido comunicado pelo controlador, **nos prazos e condições descritos nos arts. 6º e 9º deste Regulamento, respectivamente.**
>
> § 1º A ANPD poderá fixar multa diária para assegurar o cumprimento da determinação prevista no caput.

§ 2º Da decisão caberá recurso, no prazo de 3 (três) dias úteis, ao Conselho Diretor, com efeito suspensivo.

§ 3º Caso a decisão seja nos termos do § 1º, caberá pedido de reconsideração ao Conselho Diretor, no prazo de três dias, devidamente fundamentado.

§ 4º A ANPD poderá, ainda, instaurar processo administrativo sancionador para apurar o descumprimento do previsto nos arts. 6º e 9º deste Regulamento.

Proposta de nova redação para os dispositivos em pauta:

308. Após a análise das contribuições acima citadas, é apresentada a nova proposta redacional, sendo que as redações suprimidas se encontram tachadas e as inseridas em negrito, para melhor compreensão da proposta:

Seção II

Do procedimento de apuração de incidente de segurança **com dados pessoais**

Art. 15. A ANPD poderá apurar, por meio do procedimento de apuração de incidente, a ocorrência de incidentes de segurança com dados pessoais que possam acarretar risco ou dano relevante aos titulares não comunicados pelo controlador de que venha a tomar conhecimento.

§ 1º A ANPD poderá requisitar ao controlador informações para apurar a ocorrência do incidente de segurança.

§ 2º A ANPD avaliará a ocorrência do incidente que possa acarretar risco ou dano relevante aos titulares por meio dos critérios dispostos no art. 5º deste Regulamento.

Art. 16. A ANPD determinará ao controlador o envio da comunicação do incidente à Autoridade e aos titulares, quando identificar a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares de dados que não tenha sido comunicado pelo controlador**, nos prazos e condições descritos nos arts. 6º e 9º deste Regulamento, respectivamente**.

§ 1º A ANPD poderá fixar multa diária para assegurar o cumprimento da determinação prevista no *caput*.

§ 2º Da decisão caberá recurso, no prazo de 3 (três) dias úteis, ao Conselho Diretor, com efeito suspensivo.

§ ~~2º~~ **3º** A ANPD poderá, ainda, instaurar processo administrativo sancionador para apurar o descumprimento do previsto nos arts. 6º e 9º deste Regulamento.

Regulamento - Cap. V - Seção III - Do procedimento de comunicação de incidente de segurança:

309. A minuta do regulamento colocada em consulta pública tem o seguinte texto para essa seção:

Seção III

Do procedimento de comunicação de incidente de segurança

Art. 17. O procedimento de comunicação de incidente de segurança será iniciado com o recebimento da comunicação do incidente pela ANPD.

Art. 18. A ANPD poderá, a qualquer momento, realizar auditorias ou inspeções junto aos agentes de tratamento, ou determinar a sua realização, para coletar informações complementares ou validar as informações recebidas, com o objetivo de subsidiar as decisões no âmbito do processo de comunicação de incidente de segurança com dados pessoais.

Art. 19. Avaliada a gravidade do incidente, a ANPD poderá determinar ao controlador a adoção das seguintes providências para a salvaguarda dos direitos dos titulares, dentre outras:

I - ampla divulgação do incidente em meios de comunicação; ou

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

§ 1º As providências citadas no *caput* devem estar diretamente relacionadas ao incidente de segurança.

§ 2º A depender da complexidade das providências para a salvaguarda dos direitos dos titulares a serem exigidas ao controlador, as determinações poderão ser feitas em processo administrativo apartado, nos termos do art. 32 do Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador no âmbito da Autoridade Nacional de Proteção de Dados, aprovado pela Resolução nº CD/ANPD nº 1, de 28 de outubro de 2021.

§ 3º A ANPD poderá divulgar em sua página na Internet informações relativas a incidentes de segurança com dados pessoais, com o objetivo de trazer maior transparência, segurança e orientações aos titulares afetados, observados os segredos comercial e industrial.

Art. 20. A ANPD poderá determinar ampla divulgação do incidente em meios de comunicação, a ser custeada pelo controlador, para a salvaguarda dos direitos dos titulares, nos termos do art. 48, § 2º, I da LGPD, quando a comunicação realizada pelo controlador se mostrar insuficiente para alcançar parcela significativa dos titulares afetados pelo incidente.

§ 1º A ampla divulgação do incidente em meios de comunicação deverá ser compatível com a abrangência de atuação do agente de tratamento de dados e a localização dos titulares dos dados pessoais afetados no incidente.

§ 2º A ampla divulgação do incidente poderá ser viabilizada em meio físico ou digital, considerada sempre a necessidade de se atingir o maior número possível de titulares afetados, admitidos, dentre outros, os seguintes meios de veiculação:

I - mídia escrita impressa;

II - radiodifusão de sons e de sons e imagens; ou

III - transmissão de informações pela Internet.

Art. 21. Na determinação pela ANPD das medidas para reverter ou mitigar os efeitos do incidente, serão consideradas aquelas que

possam garantir a confidencialidade, a integridade, a disponibilidade e a autenticidade dos dados pessoais afetados, bem como minimizar os efeitos decorrentes do incidente para os titulares de dados.

Art. 22. A ANPD realizará o monitoramento do cumprimento das determinações e da implantação das medidas, com base em critérios de priorização.

Art. 23. A ANPD poderá instaurar processo administrativo sancionador caso o controlador não adote as medidas para reverter ou mitigar os efeitos do incidente no prazo e nas condições determinadas pela Autoridade.

Art. 24. As providências descritas no art. 19 deste Regulamento não constituem sanções ao agente regulado, sendo equiparadas às medidas decorrentes da atividade preventiva, nos termos do Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador no âmbito da Autoridade Nacional de Proteção de Dados, aprovado pela Resolução CD/ANPD nº 1, de 28 de outubro de 2021.

Contribuições recebidas:

310. Das contribuições apresentadas para este capítulo, destacam-se, pelo volume e relevância, as seguintes sugestões:

311. Um total de treze participantes sugeriu que o título do capítulo, bem como os arts. 17 a 24, fossem complementadas para refletir a terminologia "incidente de segurança com dados pessoais" do artigo 3º Inciso X, quando couber.

312. Para o art. 17, houve duas contribuições que mencionam uma preocupação quanto a tempestividade da Comunicação. Sugere-se o ajuste e inclusão para garantir que a ANPD se certifique corretamente do recebimento da comunicação, dentro dos prazos estabelecidos pelo, evitando eventual apuração de atraso e/ou ausência de envio da comunicação. Justifica-se que o marco inicial do procedimento de comunicação de incidente de segurança importará para a verificação da tempestividade da comunicação, nos termos do art. 6º deste regulamento. Pondera-se, no entanto, que caso o procedimento de submissão do formulário na plataforma de peticionamento SUPER.BR e o recebimento pela ANPD sejam interligados por um procedimento automático e instantâneo (ou quase instantâneo), não haveria problemas, a princípio. Contudo, casa haja algum tipo de atraso entre essas duas etapas, o referido artigo implicaria em um cerceamento indevido do prazo fornecido ao controlador para comunicar o incidente.

313. Outras três contribuições sugerem a menção expressa ao formulário eletrônico de comunicação do incidente, bem como ressaltam a importância de que o formulário seja ajustado ao Regulamento resultado desta Consulta Pública.

314. Sobre o art. 18, houve 26 contribuições demonstrando uma

preocupação com uma "discricionariedade excessiva" da ANPD" quanto à realização de auditorias. Como sugestão, foram encaminhadas diversas alterações no texto, como o aviso prévio ao agente de tratamento sobre a realização da auditoria, resguardo de sigilo industrial, justificativa fundamentada etc. De forma geral, recomendaram a inclusão de salvaguardas, limitando quando e como a regulamentação autorizaria a ANPD a inspecionar dados e garantindo que essas inspeções não criem maiores riscos à privacidade.

315. Ainda, foram encaminhadas três contribuições questionando a realização de auditorias no contexto de incidentes de segurança, pois segundo os participantes, as auditorias seriam uma competência apenas da fiscalização da ANPD.

316. Quanto ao art. 19, afirmou-se que, apesar de esse dispositivo estabelecer que a ANPD deverá considerar a gravidade do incidente para determinar as providências indicadas nos incisos, fato é que não há o estabelecimento, na minuta, de qualquer parâmetro para avaliação de tal gravidade. Com isso, sugeriu-se que a Autoridade evidencie qual foi sua escolha regulatória, com a inserção de parágrafo ao referido dispositivo nesse sentido. Ademais, sugeriu-se a complementação do dispositivo para que reflita a terminologia "incidente de segurança com dados pessoais" (artigo 3º, X). Veja-se:

> Art. 19……
>
> §1º A análise de gravidade do incidente será feita considerando as informações obtidas e os critérios para a definição de risco ou dano relevante ao titular nos termos do artigo 5º desta Resolução.

317. Uma contribuição questionou a pertinência do conectivo "ou" nos Incisos I e II, sugerindo que sejam cumulativos.

318. Um participante sugeriu a junção dos artigos 19 e 20, pois o art. 20 seria uma complementação ao assunto tratado no art. 19, tornando os dispositivos do art. 20 parágrafos do art. 19.

319. Sobre o art. 20, houve 12 contribuições sugerindo a alteração do dispositivo, em função do potencial gravoso ao controlador da divulgação ampla. Essa alteração busca evitar que a ampla divulgação seja determinada pela ANPD de forma corriqueira, injustificada ou excessiva e que ocorra somente quando não houver alternativa viável para alcançar os titulares afetados. Segue a redação sugerida:

> Art. 20. A ANPD poderá determinar ampla divulgação do incidente em meios de comunicação, a ser custeada pelo controlador, para a salvaguarda dos direitos dos titulares, nos termos do art. 48, § 2º, I da LGPD, quando:
>
> I - comprovadamente a comunicação realizada pelo controlador se mostrar insuficiente para alcançar parcela significativa dos titulares afetados pelo incidente; e

> II - a ampla divulgação do incidente em meios de comunicação for a única forma viável para alcançar os titulares afetados".

320. Ainda quanto ao art. 20, por meio de 8 contribuições, foi sugerida a exclusão dos incisos previstos e a alteração do dispositivo para que conste a seguinte redação:

> §2º A ampla divulgação do incidente poderá ser viabilizada em meio físico ou digital, considerada sempre a necessidade de se atingir o maior número possível de titulares afetados.

321. Houve, também, três contribuições que questionam a indefinição da expressão "parcela significativa" inscrita no caput do art. 20, sendo que, em uma delas, sugere-se a substituição pelo termo "metade".

322. Já para o art. 21, quatro participantes sugeriram a supressão da palavra "autenticidade", já que o conceito de "autenticidade" não está previsto na LGPD e nem nas orientações relativas à segurança da informação já disponibilizadas pela ANPD. Além disso, foi sugerida a inserção da expressão "observadas as boas práticas setoriais", por meio de três contribuições. Por fim, houve sugestão de indicação de prazo para o atendimento da determinação. Esse prazo, de acordo com a contribuição, deveria ser estabelecido de forma faseada, se necessário, considerando também a eventual insuficiência de recursos ou disponibilidade técnica por parte do Controlador.

323. Quanto ao art. 22 da minuta, em cinco contribuições, questionou-se quais são os critérios de priorização. Destaca-se a obrigatoriedade da transparência na divulgação dos critérios determinados e o respeito ao contraditório e a ampla defesa no curso do processo administrativo.

324. Para o art. 23 da minuta, sugeriu-se a inclusão da expressão "diretamente relacionados ao incidente" na redação do dispositivo, para alinhamento com a redação extraída do § 1º do art. 19. Algumas das contribuições destacaram a atuação responsiva da ANPD. Assim, seria importante que as determinações da autoridade levassem em conta as especificidades do caso concreto, bem como do próprio agente de tratamento. No mesmo sentido, mostrou-se preocupação de se mencionar expressamente o atendimento ao devido processo legal. Houve, ainda, a sugestão de inserção de um parágrafo que mencione o incentivo à conciliação direta entre o controlador e o titular, de que trata o § 7º do art.52 da LGPD.

325. Sobre o art. 24, sugeriu-se acrescentar os artigos em que há previsão específica das medidas decorrentes de atividade preventiva, em razão da própria redação utilizada pela Resolução CD/ANPD nº 1, de 28 de outubro de 2021, alterada pela Resolução CD/ANPD nº 4, de 24 de fevereiro de 2023. Além disso, sugeriu-se a inclusão de menção expressa ao artigo 20, que também dispõe sobre a ampla divulgação do incidente de segurança em atendimento à determinação da ANPD. Por fim, sugeriu-se a supressão do artigo, tendo em vista que as medidas preventivas já constam no

Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador.

Análise:

326. Sobre o art. 17, quanto a tempestividade da comunicação, o texto atual coloca o início do procedimento como o recebimento da comunicação do incidente pela ANPD. Há uma preocupação quanto a um eventual atraso entre o envio pelo controlador e o recebimento pela ANPD. De fato, atualmente os dois eventos acontecem de forma quase simultânea, de forma que não se vislumbram diferenças entre envio e recebimento. Entende-se que os casos de problema no sistema disponibilizado para envio e recebimento correspondem a excepcionalidades que poderão ser analisadas caso a caso, com a confirmação da indisponibilidade ou de outros problemas semelhantes com o setor responsável pelo funcionamento do sistema utilizado. Quanto a mencionar o uso do formulário expressamente no texto, acatou-se a sugestão, de modo a assegurar a forma de utilização do formulário eletrônico como uma obrigatoriedade. Foi inserido, então, o parágrafo único que limita a comunicação do incidente na forma determinada no sítio eletrônico da ANPD. Em relação ao ajuste do conteúdo do formulário em si, em conformidade com o texto do regulamento, a CGF reconhece a existência dessa necessidade e prevê o ajustamento, conforme os termos do texto devidamente aprovado e publicado.

327. Quanto ao art. 18, a realização de auditorias é discricionária da ANPD, conforme a conveniência e oportunidade no contexto do caso concreto, motivo por que não cabe impor limites à sua realização nem aos seus objetivos por meio do Regulamento em causa, já que ela é, por natureza, pautada na legalidade e na competência das atribuições funcionais do órgão. Tal atividade está prevista no Inciso XVI do Artigo 55-J da LGPD, com observância aos segredos comercial e industrial, conforme pontua o Inciso II do mesmo artigo. Embora o texto da minuta não expresse de forma explícita o âmbito de uma auditoria nem o que ela implicaria, a ação da ANPD é pautada em princípios constitucionais. Neste sentido, conforme doutrina do TCU, o princípio da razoabilidade dispõe, essencialmente, que deve haver uma proporcionalidade entre os meios de que se utilize a Administração e os fins que ela tem que alcançar, e mais, que tal proporcionalidade não deve ser medida diante dos termos frios da lei, mas diante do caso concreto. A apuração de incidentes de segurança é uma das atribuições da Coordenação-Geral de Fiscalização, de acordo com os Incisos VII e XXII da Portaria nº 1, de 2021 (RIANPD), e corresponde também a uma atividade de fiscalização em sentido amplo.

328. Sobre o art. 19, importa registrar que sua escolha regulatória foi a aplicação das determinações disposta no art. 48, § 2º após análise da gravidade do incidente comunicado, avaliar a adequação das providências a serem determinadas conforme o nível de gravidade identificado. No Relatório de Impacto Regulatório (pp.59-60), a opção escolhida foi descrita da seguinte

forma:

> Nessa alternativa, a determinação de providências, caso necessário, é aplicada após **a análise do incidente**, que o**corre com base nas informações enviadas e nos critérios para a definição de risco ou dano relevante ao titular**.
>
> Nesse sentido, **a providência de determinação de ampla divulgação em meios de comunicação ocorrerá quando a comunicação direta e individualizada se mostrar inviável e quando a comunicação realizada pelo controlador se mostrar insuficiente para alcançar parcela significativa dos titulares afetados pelo incidente**. A divulgação poderá ser viabilizada em meio físico ou digital, considerada sempre a necessidade de se atingir o maior número possível de titulares afetados, admitidos os meios de veiculação, tais como: mídia escrita impressa, radiodifusão de sons e de sons e imagens ou Internet.
>
> Já a determinação de medidas para reverter ou mitigar os efeitos do incidente é aplicada para garantir a confidencialidade, integridade e disponibilidade dos dados pessoais afetados, bem como as medidas para minimizar os efeitos decorrentes do incidente. (grifo nosso)

329. Em reação às contribuições quanto aos critérios para análise da gravidade do incidente, é salutar esclarecer na minuta a escolha regulatória de que a análise de gravidade ocorrerá com base nas informações enviadas e nos critérios para a definição de risco ou dano relevante ao titular, conforme sugerido em uma delas.

330. Ainda sobre o art. 19, de fato, o uso do "ou" ao final do primeiro inciso gera dúvidas quanto à intepretação e aplicabilidade dos incisos, isto é, se são aplicáveis alternativamente ou cumulativamente. Ademais, o § 2º do art. 48 da LGPD faz uso da conjunção "e". Desta forma, deferiu-se a sugestão, passando a constar a conjunção “e”.

331. Por fim, acatou-se que a proposta da contribuição sobre transformar o art. 20 em parágrafos do art. 19, uma vez que os dispositivos do art. 20 tratam de aspectos complementares à norma enunciada no caput do art. 19, conforme orienta a alínea "c" do inciso III do art. 11 da Lei complementar nº 95, de 26 de fevereiro de 1998. Importante sublinhar que a ampla divulgação trazida no dispositivo do art. 20 trata-se da adoção de um mecanismo procedimental voltado à minimização dos efeitos negativos ocasionados por um incidente de segurança. Complementarmente, a ampla divulgação aí descrita funciona, ainda, como medida de transparência e como *munus* do exercício pelo titular de dados de seus direitos e a preservação dos fundamentos insculpidos na LGPD, em especial a autodeterminação informativa. Diferentemente, a sanção administrativa da publicização da infração prevista no inciso IV do art. 52 da LGPD tem, por óbvio, natureza sancionatória e seu objeto é a conduta infrativa, não a ocorrência de um incidente.

332. Já quanto ao art. 20, entendeu-se desnecessária as

condicionantes "comprovadamente" e "única forma viável", uma vez que o inciso II do art. 50 da Lei nº 9784, de 1999, estabelece o dever de motivar atos administrativos que imponham ou agravem deveres, encargos ou sanções. Além disso, quanto à expressão “parcela significativa”, em que pese careça de definição, o estabelecimento de certo quantitativo pode não ter efetividade para a análise do caso concreto, de modo que é preferível que a análise do atendimento a "parcela significativa" seja feita em conjunto com outros fatores.

333. Quanto à contribuição para alteração ou exclusão do §2º do art. 20, concluiu-se pela manutenção do dispositivo.

334. O art. 9º trata de uma medida ordinária em sede de comunicação de incidente ao titular. É uma medida aplicada a qualquer caso em que se configura risco ou dano relevante.

335. Por sua vez, o art. 20, §2º está sujeito a uma condição incerta, em que a ANPD poderá ou não determinar medida de ampla divulgação para a salvaguarda dos direitos dos titulares, nos termos do art. 48, § 2º, I, da LGPD, quando a comunicação realizada pelo controlador se mostrar insuficiente para alcançar parcela significativa dos titulares afetados pelo incidente.

336. Em relação ao art. 21, embora "autenticidade" seja um conceito importante para a segurança cibernética, tal como "não negação", os conceitos basilares são a confidencialidade, a integridade e a disponibilidade. Além do já explicitado na Nota Técnica nº 12/2023/CGN/ANPD (4012432), do parágrafo 239 ao 254, esses são os conceitos aos quais a LGPD e o Guia sobre segurança da informação para agentes de tratamento de pequeno porte fazem referência. Destarte, para uniformizar este regulamento com as normas e orientações já existentes, concordou-se em suprimir o conceito "autenticidade" do art. 21. Quanto ao conceito de "boa prática", já está previsto no art. 49 da LGPD. Dessa forma, a sugestão do participante não trouxe nenhuma inovação quanto ao que já é esperado dos agentes de tratamento e da ANPD. Por fim, quanto à sugestão de indicação de prazo para o atendimento da determinação, esclarece-se que, a exemplo do art. 34 da Resolução CD/ANPD nº 1, de 28 de outubro de 2021, que trata sobre solicitação de regularização e informe, o prazo estipulado ao agente de tratamento não é fixo, e mensurado de acordo com o caso concreto. Assim, não é viável estipular um prazo fixo nesta norma.

337. Quanto ao art. 21, foi modificado para parágrafo do art. 19 pela mesma motivação.

338. Já sobre o art. 22, quanto a transparência dos critérios de priorização, os arts. 21 e 22 da Resolução CD/ANPD Nº 1, de 28 de outubro de 2021, preveem o mapa de temas prioritários como instrumento de estudo e planejamento da atividade de fiscalização da ANPD, bem como os critérios risco, gravidade, atualidade e relevância para priorização. Deste modo, entende-se desnecessária previsão semelhante no Regulamento em causa.

339. Quanto ao art. 23, quanto à sugestão para se mencionar a expressão "diretamente relacionados ao incidente", em relação às medidas para reverter ou mitigar os efeitos do incidente, ela já está contemplada no § 1º do art. 19.

340. Quanto à contribuição para inserção de um parágrafo no art. 23 que mencione o incentivo à conciliação direta entre o controlador e o titular, de que trata o § 7º do art. 52 da LGPD, observa-se que a conciliação "direta" é medida entre atores privados, isto é, o controlador e o titular de dados, tal como ocorre entre consumidores e fornecedores ou prestadores de serviço. O objetivo da norma é disciplinar a comunicação de incidentes de segurança com dados pessoas à ANPD e ao titular. Caso seja situação de conciliação direta, esta ocorreria após o titular tomar conhecimento de vazamentos individuais ou os acessos não autorizados de que trata o caput do art. 46 da LGPD.

341. Considerando as contribuições relativas ao art. 24, cumpre esclarecer que a ANPD adota o modelo de regulação responsiva, em que o objetivo não é punir e sim, prevenir, cessar ou mitigar danos aos titulares de dados pessoais. No caso de haver necessidade de instauração de processo sancionador, todas as evidências são criteriosamente analisadas, inclusive eventuais justificativas por parte do agente de tratamento, antes de proferir uma decisão a favor ou contra a lavratura de atos punitivos, conforme o disposto na Resolução CD/ANPD nº 1, de 28 de outubro de 2021 e na LGPD. Além disso, entendeu-se não ser conveniente mencionar apenas os artigos 30 e 31 da Resolução CD/ANPD nº 1, de 28 de outubro de 2021, pois outros artigos podem ser relevantes no caso concreto, como o relacionado ao plano de conformidade, por exemplo.

<u>Proposta de nova redação para os dispositivos em pauta:</u>

342. Após a análise das contribuições acima citadas, é apresentada a nova proposta redacional, sendo que as redações suprimidas se encontram tachadas e as inseridas em negrito, para melhor compreensão da proposta. A CGN alterou a expressão “a ser custeada pelo controlar” por "às expensas do controlador", por ser mais econômica, no caput do art. 20, renumerado para § 3º. Veja-se:

> Seção III
>
> Do procedimento de comunicação de incidente de segurança **com dados pessoais**
>
> Art. 17. O procedimento de comunicação de incidente de segurança **com dados pessoais** será iniciado com o recebimento da comunicação do incidente pela ANPD.
>
> **Parágrafo único. A comunicação do incidente será recebida exclusivamente por meio de canal específico, conforme orientação publicada no sítio eletrônico da ANPD.**
>
> Art. 18. A ANPD poderá, a qualquer momento, realizar auditorias ou

inspeções junto aos agentes de tratamento, ou determinar a sua realização, para coletar informações complementares ou validar as informações recebidas, com o objetivo de subsidiar as decisões no âmbito do processo de comunicação de incidente de segurança com dados pessoais.

Art. 19. **Após avaliar** ~~Avaliada~~ a gravidade do incidente **de segurança com dados pessoais**, a ANPD poderá determinar ao controlador a adoção das seguintes providências para a salvaguarda dos direitos dos titulares, ~~dentre outras~~ **tais como:**

I - ampla divulgação do incidente em meios de comunicação; ~~ou~~ **e**

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

§ 1º ~~As providências citadas no *caput* devem estar diretamente relacionadas ao incidente de segurança~~. **A gravidade do incidente será avaliada com base nas informações obtidas e nos critérios para a definição de risco ou dano relevante ao titular de que trata o art. 5º deste Regulamento.**

§ 2º ~~A depender da complexidade das providências para a salvaguarda dos direitos dos titulares a serem exigidas ao controlador, as determinações poderão ser feitas em processo administrativo apartado, nos termos do art. 32 do Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador no âmbito da Autoridade Nacional de Proteção de Dados, aprovado pela Resolução nº CD/ANPD nº 1, de 28 de outubro de 2021.~~ **As providências citadas no *caput* devem estar diretamente relacionadas ao incidente.**

§ 3º **A ANPD poderá divulgar em seu sítio eletrônico informações estatísticas agregadas relativas aos incidentes de segurança com dados pessoais que lhe forem comunicados pelos agentes como medida de transparência ativa.** ~~A ANPD poderá divulgar em sua página na Internet informações relativas a incidentes de segurança com dados pessoais, com o objetivo de trazer maior transparência, segurança e orientações aos titulares afetados, observados os segredos comercial e industrial.~~

~~Art. 20~~ **§ 4º** A ANPD poderá determinar ampla divulgação do incidente em meios de comunicação, **às expensas do controlador** ~~a ser custeada pelo controlador~~, para a salvaguarda dos direitos dos titulares, nos termos do art. 48, § 2º, I, da LGPD, quando a comunicação realizada pelo controlador se mostrar insuficiente para alcançar parcela significativa dos titulares afetados pelo incidente.

§ ~~1~~ **5º** A ampla divulgação do incidente em meios de comunicação deverá ser compatível com a abrangência de atuação do agente de tratamento de dados e a localização dos titulares dos dados pessoais afetados no incidente.

§ ~~2~~ **6º** A ampla divulgação do incidente poderá ser viabilizada em meio físico ou digital, considerada sempre a necessidade de se atingir o maior número possível de titulares afetados, admitidos, ~~dentre outros,~~ os seguintes meios de veiculação:

I - mídia escrita impressa;

II - radiodifusão de sons e de sons e imagens; ou

III - transmissão de informações pela Internet.

~~Art. 21~~. **§ 7º A ampla divulgação do incidente não se confunde com a publicização expressa no art. 52, IV, da LGPD, referente às sanções administrativas.**

§ 8º Na determinação pela ANPD das medidas para reverter ou mitigar os efeitos do incidente, serão consideradas aquelas que possam garantir a confidencialidade, a integridade~~,~~ **e** a disponibilidade ~~e a autenticidade~~ dos dados pessoais afetados, bem como minimizar os efeitos decorrentes do incidente para os titulares de dados.

~~Art. 22. A ANPD realizará o monitoramento do cumprimento das determinações e da implantação das medidas, com base em critérios de priorização.~~

Art. ~~23~~ **20**. A ANPD poderá instaurar processo administrativo sancionador caso o controlador não adote as medidas para reverter ou mitigar os efeitos do incidente **de segurança com dados pessoais** no prazo e nas condições determinadas pela Autoridade.

Art. ~~24~~ **21.** As providências descritas no art. 19 deste Regulamento não constituem sanções ao agente regulado, sendo equiparadas às medidas decorrentes da atividade preventiva, nos termos do Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador no âmbito da Autoridade Nacional de Proteção de Dados, aprovado pela Resolução CD/ANPD nº 1, de 28 de outubro de 2021.

Regulamento - Cap. V - Seção IV - Da extinção do processo de comunicação de incidente segurança com dados pessoais:

343. A minuta do regulamento colocada em consulta pública tem o seguinte texto para essa seção:

Seção IV

Da extinção do processo de comunicação de incidente de segurança

Art. 25. O processo de comunicação de incidente de segurança com dados pessoais poderá ser declarado extinto nas seguintes hipóteses:

I - Ao final do procedimento de apuração de incidente de segurança:

a) caso não sejam identificadas pela ANPD evidências suficientes da ocorrência do incidente, ressalvada a possibilidade de reabertura caso surjam fatos novos;

b) caso a ANPD considere que o incidente não possui potencial para acarretar risco ou dano relevante aos titulares de dados; ou

c) caso o incidente não envolva dados pessoais.

II - No curso do procedimento de comunicação de incidente de segurança:

a) se a ANPD considerar que o incidente não acarreta risco ou dano

relevante aos titulares de dados; ou

b) que não sejam necessárias medidas adicionais para mitigação ou reversão dos efeitos gerados.

Parágrafo único. Na hipótese da alínea b, do inciso I, mesmo com a decisão da extinção do processo de comunicação de incidente de segurança com dados pessoais, a ANPD poderá determinar a adoção de medidas de segurança com o intuito de salvaguardar os direitos dos titulares.

Contribuições Recebidas:

344. Das 57 contribuições apresentadas para esta Seção, destacam-se, pelo volume e relevância, as sugestões de ajustes redacionais relativamente aos incisos I e II do art. 25, abaixo consolidadas:

I - Sugestão de redação mais esclarecedora no inciso I, alínea (a): Entende-se que se o fato é novo e significativo, mas é relacionado ao mesmo incidente, faz sentido a reabertura, desde que garantidos novamente o contraditório e a ampla defesa ao controlador. No mais, vale a ANPD esclarecer o que se entende por fatos novos, de que forma estes devem ser apresentados e até qual prazo, por exemplo. Isso porque se não forem impostos alguns limites, o rito poderá gerar insegurança jurídica.

II - Sugestão de nova redação ao inciso I, alínea (a): Sugestão de redação: "(...) a) caso não sejam identificadas pela ANPD evidências suficientes da ocorrência do incidente, ressalvada a possibilidade de reabertura caso surjam fatos novos, no período máximo de seis meses contados da data de confirmação da ocorrência do incidente.

III - Sugestão de nova redação ao inciso I, alínea (a): Sugestão de redação: "(...) Sugestão de alteração: a) caso não sejam identificadas pela ANPD evidências suficientes da ocorrência do incidente, ressalvada a possibilidade de reabertura caso surjam fatos novos, no período máximo de três anos contados da data de confirmação da ocorrência do incidente;

IV - Sugestão de nova redação ao inciso I, alínea (a): Sugestão de redação: "(...) a) caso não sejam identificadas pela ANPD evidências suficientes da ocorrência do incidente, ressalvada a possibilidade de reabertura caso surjam fatos novos observando-se o lapso temporal de até cinco anos a contar do registro das informações relativas ao incidente pelo controlador, nos termos previstos no art. 10 deste Regulamento;
Sugestão de nova redação ao inciso I, alíneas (a) e (b): "(...) a) caso não sejam identificadas pela ANPD evidências suficientes

da ocorrência do incidente, ressalvada a possibilidade de reabertura exclusivamente na hipótese de ocorrência de fatos novos diretamente relacionados ao incidente de segurança; b) caso a ANPD considere que o incidente não possui potencial para acarretar risco ou dano relevante aos titulares de dados nos termos do Art. 5º deste Regulamento".

V - Sugestão de nova redação ao inciso I, alínea (c): Sugere-se esclarecer se essa hipótese de extinção será realizada no início do procedimento como forma de indeferimento ou será apurado apenas no fim.

VI - Sugestão de inclusão de alínea (d) no inciso I: Sugestão de redação: "(...) d) Quando demonstrado pelo controlador à ANPD de forma fundamentada que o procedimento de comunicação de incidente de segurança com dados pessoais pode ser extinto."

VII - Sugestão de inclusão de alíneas (d, e, f) no inciso I: Sugestão de redação: "(...) d) quando os controladores provarem que não realizaram o tratamento de dados pessoais que lhes é atribuído; e) quando não houve violação à legislação de proteção de dados; ou f) quando o dano é decorrente de culpa exclusiva do titular dos dados ou de ato ilícito de terceiro."

VIII - Sugestão de inclusão de alínea EXTRA inciso I: Sugestão de redação 1: "(...) d) caso adotadas todas as medidas aplicáveis ao gerenciamento do incidente pelo controlador ou que não sejam necessárias medidas adicionais para mitigação ou reversão dos efeitos gerados." Sugestão de redação 2: "(...) d) caso o controlador tenha implementado medidas adicionais suficientes para mitigação ou reversão dos riscos ou danos relevantes identificados (ou dos efeitos gerados); Sugestão de redação 3: "(...) d) Quando demonstrado pelo controlador à ANPD de forma fundamentada que o procedimento de comunicação de incidente de segurança com dados pessoais pode ser extinto."

IX - Sugestão de nova redação ao inciso II, alíneas (a) e (b): Sugestão de redação 1: "(...) a) Caso a ANPD considere que o incidente não possui potencial para acarretar risco ou dano relevante aos titulares de dados (nos termos do art. 5º deste Regulamento); b) Caso não sejam necessárias medidas adicionais para mitigação ou reversão dos efeitos gerados pelo incidente. Sugestão de redação 2: "(...) a) se a ANPD considerar que o incidente não possui potencial para acarretar risco ou dano relevante aos titulares de dados; Sugestão de redação 3: "(...) b) que não sejam necessárias

medidas adicionais para mitigação ou reversão dos efeitos gerados pelo incidente de segurança."

345. Quanto ao parágrafo único do art. 25, quinze contribuições sugeriram sua exclusão ou nova redação nos seguintes termos:

I - Sugestão de redação 2: "(...) Parágrafo único. Na hipótese da alínea b, do inciso I, mesmo com a decisão da extinção do processo de comunicação de incidente de segurança com dados pessoais, a ANPD poderá determinar a adoção de medidas de segurança que considerem o porte e as características de negócio da empresa, caso o controlador não tenha ainda realizado, com o intuito de salvaguardar os direitos dos titulares, na forma do art. 46 da LGPD".

II - Sugestão de redação 3: "(...) Parágrafo único. Na hipótese da alínea b, do inciso I, a ANPD poderá determinar a adoção de medidas de segurança com o intuito de salvaguardar os direitos dos titulares como condição para extinção do processo de comunicação de incidente de segurança com dados pessoais."

III - Sugestão de redação 1: "(...) Parágrafo único. Na hipótese da alínea b, do inciso I, mesmo com a decisão da extinção do processo de comunicação de incidente de segurança com dados pessoais, a ANPD poderá sugerir a adoção de medidas de segurança, diretamente relacionadas ao incidente, com o intuito de salvaguardar os direitos dos titulares.

346. Por fim, três contribuições sugeriram inclusão de parágrafo extra com a seguinte redação:

"(...) §2º. Incide a prescrição no processo de comunicação de incidente de segurança paralisado por mais de três anos, pendente de julgamento ou despacho, cujos autos serão arquivados de ofício ou mediante requerimento da parte interessada, sem prejuízo da apuração da responsabilidade funcional decorrente da paralisação, se for o caso."

Análise:

347. A partir da análise das 57 contribuições acima citadas, verifica-se que restou esclarecido ao público que se o fato é novo e significativo, mas é relacionado ao mesmo incidente, faz sentido a reabertura do processo, desde que garantidos novamente o contraditório e a ampla defesa ao controlador.

348. Por sua vez, entenderam os contribuintes que se não forem impostos alguns limites, especialmente quanto a ausência de definição de lapso temporal na norma, o rito poderá gerar insegurança jurídica.

349. Todavia, tal argumento não merece prosperar à medida que as disposições relativas aos marcos temporais incidentes sobre a presente norma, inclusive os prazos prescricionais, já se encontram legalmente previstos e serão exercidos pela ANPD conforme os termos de seu poder de polícia.

350. Assim, a equipe de projeto acatou apenas as sugestões relativas ao ajuste redacional do inciso I, alínea "b" e do parágrafo único para esclarecer que a ANPD poderá determinar, durante o processo de comunicação, a adoção de medidas de segurança adicionais que sejam diretamente relacionadas ao acidente.

351. Especificamente quanto a sugestão de inclusão da expressão "nos termos do art. 5º deste Regulamento", a equipe de projeto concordou que o presente ajuste redacional no inciso I, pretende:

> I - manter a coerência com a redação extraída do art. 19, §1º, limitando-se assim a fatos novos que estejam diretamente relacionados ao incidente tratado no caso;
>
> II - garantir ao controlador que o processo somente será reaberto na exclusiva hipótese de fato novo, afastando-se interpretações amplas que possa abarcar situações distintas.

Proposta de nova redação para os dispositivos em pauta:

352. Após a análise das contribuições acima citadas, é apresentada a nova proposta redacional, sendo que as redações suprimidas se encontram tachadas e as inseridas em negrito, para melhor compreensão da proposta, veja-se:

> Art. ~~25~~ **22**. O processo de comunicação de incidente de segurança com dados pessoais poderá ser declarado extinto nas seguintes hipóteses:
>
> I - Ao final do procedimento de apuração de incidente de segurança:
>
> (...) b) caso a ANPD considere que o incidente não possui potencial para acarretar risco ou dano relevante aos titulares de dados, **nos termos do art. 5º deste Regulamento**; ou
>
> Parágrafo único. Na hipótese da alínea b, do inciso I, mesmo com a decisão da extinção do processo de comunicação de incidente de segurança com dados pessoais, a ANPD poderá determinar a adoção de medidas de segurança, **diretamente relacionadas ao incidente,** com o intuito de salvaguardar os direitos dos titulares.

Regulamento - Cap. VI - Das disposições finais:

353. A minuta do regulamento colocada em consulta pública tem o seguinte texto para essa seção:

CAPÍTULO VI

DAS DISPOSIÇÕES FINAIS

Art. 26. Ao entrar em vigor este Regulamento, suas disposições se aplicarão aos processos de comunicação de incidentes de segurança em curso, respeitados os atos já praticados.

Contribuições Recebidas:

354. O artigo pretende estabelecer a retroatividade do regulamento aos processos de comunicação de incidentes, respeitados os "atos já praticados".

355. Considerando a natureza complexa do ato de comunicação de incidente de segurança, que envolve várias etapas e que a norma impõe aos atos novos requisitos e prazos, as sugestões dadas pelos participantes se concentraram na necessidade de ser adotada uma redação mais detalhada a fim de conferir maior segurança jurídica aos administrados.

356. Assim, das contribuições apresentadas para este Capítulo Final, destacam-se, pelo volume e relevância, as vinte sugestões que propuseram que a presente norma tenha efeito ex-nunc, ou seja, valendo apenas para os novos processos a partir da data da publicação e não para os em curso.

357. Segundo os participantes, o Regulamento traz diversas obrigações e procedimentos que não eram obrigatórios aos agentes de tratamento e sequer eram mencionados pela LGPD e, por isso, estabelecer que as disposições do Regulamento serão aplicáveis a todos os processos de comunicação que já foram enviados à Autoridade implicaria na necessidade de os controladores complementarem as comunicações que estão em curso perante a Autoridade para que contemplem os novos requisitos indicados no Regulamento.

358. Conforme entendimento das citadas contribuições, a retroatividade pode exigir ajustes e reanálise dos processos tanto pela parte dos agentes de tratamento de dados quanto pela própria ANPD sobre incidentes comunicados antes da vigência do regulamento.

359. Ou seja, tal decisão, além de conferir insegurança jurídica, demandaria um esforço desproporcional tanto dos agentes, quanto da ANPD, que terá de avaliar as todas as complementações realizadas.

360. Assim, foram propostos os seguintes ajustes redacionais:

I - Sugestão de redação 2: "(...) As disposições previstas neste Regulamento se aplicarão aos processos de comunicação de incidentes de segurança comunicados a partir de sua entrada em vigor.

II - Sugestão de redação 1: "(...) As disposições deste Regulamento se aplicarão aos processos de comunicação de incidentes de segurança instaurados a partir de sua

publicação.”

III - Sugestão de redação 3: “(...) Ao entrar em vigor este Regulamento, suas disposições se aplicarão aos novos processos de comunicação de incidentes de segurança e, no que couber, aos processos em curso, respeitados os atos já praticados. Por fim, importante destacar que, por ocasião da publicação deste Regulamento, o Formulário de Comunicação de Incidente de Segurança deverá ser revisto e equalizado, tanto com relação à terminologia quanto aos prazos e às informações obrigatórias definidas pela Autoridade.

IV - Sugestão de redação 4: “(...) Ao entrar em vigor este Regulamento, suas disposições se aplicarão aos processos de comunicação de incidentes de segurança em curso, respeitados os atos já praticados, sobre os quais não incidirão as disposições deste Regulamento.

V - Sugestão de redação 5: “(...) “Art. 26. Ao entrar em vigor este Regulamento, suas disposições se aplicarão aos processos de comunicação de incidentes de segurança em curso, no que for aplicável, respeitados os atos já praticados.”

VI - Sugestão de redação 6: “(...) Ao entrar em vigor este Regulamento, suas disposições se aplicarão aos processos de comunicação de incidentes de segurança em curso, respeitados os atos já praticados, sobre os quais não incidirão as disposições deste Regulamento.”

Análise:

361. Verificando as sugestões acima transcritas e os argumentos oferecidos, especialmente quanto à necessidade de esclarecer que não haverá retroatividade na aplicação do Regulamento aos atos já praticados, aplicando-se o princípio do *tempus regit actum*, extraído do art. 6º, caput, da LINDB e do art. 5º, inciso XXXVI, da CF/88, para o qual a validade de atos jurídicos deve observar o ordenamento jurídico à época da prática dos referidos atos, a equipe de projeto entendeu que, de fato, a redação do artigo deve esclarecer que o Regulamento é aplicável apenas às comunicações de incidente realizadas a partir da data de sua publicação.

362. Ademais, no comparativo entre os anos de 2021 e 2022, verifica-se um crescimento significativo de 56% dos comunicados de incidente de segurança recebidos pela ANPD - o que deve aumentar exponencialmente com a publicação deste Regulamento, ampliando, por consequência, o percentual de represamento da análise de processos de comunicados de incidentes de segurança atual - motivo pelo qual a equipe de projeto verificou um risco potencial de "aumento significativo do acervo processual e eventual prescrição de processos em razão de limitações operacionais”, caso seja mantida a redação original.

Proposta de nova redação para os dispositivos em pauta:

363. Após a análise das contribuições acima citadas, é apresentada a nova proposta redacional, sendo que as redações suprimidas se encontram tachadas e as inseridas em negrito, para melhor compreensão da proposta, veja-se:

> Art. 26. ~~Ao entrar em vigor este Regulamento, suas disposições se aplicarão aos processos de comunicação de incidentes de segurança em curso, respeitados os atos já praticados.~~ **As disposições previstas neste Regulamento aplicar-se-ão aos processos de comunicação de incidentes de segurança comunicados a partir de sua entrada em vigor.**

3. CONSIDERAÇÕES FINAIS

364. Após análise das contribuições apresentadas durante a consulta pública e a audiência pública, realizadas dentro do prazo de 45 dias, cabe destacar que muitas destas contribuições amadureceram o debate entre os integrantes da equipe de projeto e, de certo modo, suscitaram algumas dúvidas pertinentes aos temas avaliados.

365. Desta forma, em que pese tenha-se sugerido que algumas das contribuições não fossem acatadas e incorporadas, neste momento, na proposta de ato normativo, ressalta-se que a qualidade do teor e do mérito apresentado nessas contribuições orientará o monitoramento e a Avaliação do Resultado Regulatório (ARR) do regulamento que entrará em vigor.

366. Sendo assim, a sociedade poderá, conjuntamente com a ANPD, avaliar se os objetivos propostos pela intervenção regulatória estão sendo atingidos ou se haverá necessidade de revisão pontual ou, até mesmo, integral da norma.

367. Nesse sentido, não só a aplicação do regulamento e o seu monitoramento orientará a necessidade de possível revisão no âmbito da ARR, pois a participação da sociedade e dos atores envolvidos também é uma ferramenta de suma importância a ser utilizada no processo de regulamentação da ANPD.

4. CONCLUSÃO

368. Tendo em vista a análise das contribuições apresentadas pela sociedade no âmbito da consulta pública e da audiência pública realizada ao longo desta Nota Técnica, apresenta-se sugestão de nova proposta de resolução que aprova o Regulamento de Comunicação de Incidentes de Segurança.

369. Assim, sugere-se o encaminhamento dos autos à Procuradoria

Federal Especializada junto à ANPD para análise da minuta de resolução (SEI nº 4850046), especialmente quanto à possibilidade de não inclusão de conteúdos dispostos nos incisos do § 1º do art. 48, apesar de a LGPD indicá-los como elementos mínimos a serem mencionado na comunicação ao titular.

5. ANEXOS

Minuta do RCIS com marcas no formato pdf (SEI nº 4850046)
Minuta do RCIS com marcas no formato word (SEI nº 4850021)
Minuta do RCIS limpa no formato word (SEI nº 4842488)

À consideração superior.

FABÍOLA SOARES PINTO
Empregada Pública em exercício na ANPD

RAFAEL ALVES LOURENÇO

Analista Técnico da SUSEP em exercício na ANPD

MARIANA TALOUKI

Coordenadora de Normatização - CON1

De acordo. Encaminhe-se o presente processo à Procuradoria Federal Especializada junto à ANPD.

RODRIGO SANTANA DOS SANTOS
Coordenador-Geral de Normatização

_____

[1] Disponível em: https://www.gov.br/participamaisbrasil/regulamento-de-comunicacao-de-incidente-de-seguranca-com-dados-pessoais. Acesso em: 29 jun. 2023.

[2] A equipe de projeto que analisou as contribuições foi composta pelos servidores Fabíola de Gabriel Soares Pinto (CGN), Cleórbete Santos (CGTP), Mariana Herminia da Costa (CGF), Maria Carolina Ferreira da Silva (CGTP), Patrick Marques Trompowsky (CGF) e Rafael Alves Lourenço (CGN), sob coordenação de Mariana Almeida de Sousa Talouki, conforme Despacho CGN - Equipe de Projeto (SEI nº 4383766), no âmbito do Processo ANPD nº 00261.000098/2021-67.

[3] Disponível em: http:// https://www.youtube.com/watch?v=5KCIVpnmnsA&ab_channel=anpdgov
[4] Disponível em https://gdpr-text.com/pt/. Acesso em: 20 dez 2023.
[5] https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/d9936.htm. Acesso em: 20 dez 2023.
[6] https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm. Acesso em: 20 dez 2023.
[7] https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-personal-data-breach-notification-under_en. Acesso em: 20 dez 2023.

Documento assinado eletronicamente por **Rodrigo Santana dos Santos**, **Coordenador(a)-Geral**, em 21/12/2023, às 14:59, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Mariana Almeida de Sousa Talouki**, **Coordenador(a)**, em 21/12/2023, às 15:30, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Fabíola de Gabriel Soares Pinto**, **ANPD - Autoridade Nacional de Proteção de Dados**, em 21/12/2023, às 15:47, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º, do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade do documento pode ser conferida informando o código verificador **4842505** e o código CRC **171C4595** no site: https://super.presidencia.gov.br/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0