Brasília, 15 de junho de 2023

Ao Senhor
Rodrigo Santana dos Santos
Coordenador-Geral de Normatização
Autoridade Nacional de Proteção de Dados (ANPD)
normatizacao@anpd.gov.br

Assunto: Consulta Pública sobre o Regulamento de Comunicação de Incidente de Segurança com Dados Pessoais. Comentários e sugestões a artigos específicos da minuta de Regulamento.

Senhor Coordenador,

1. A Associação Latino-Amerinca de Internet (ALAI) oferece suas contribuições à Consulta Pública nº 01/2023/ANPD, de 02.05.2023, e sugere pontos a serem considerados pela Autoridade Nacional de Proteção de Dados (ANPD) na elaboração de minuta de regulamento sobre Comunicação de Incidente de Segurança com Dados Pessoais.

2. Informo que os textos abaixo foram inseridos na Plataforma + Brasil.

3. Seguimos disponíveis para diálogo e refinamento das ideias aqui expostas.

Respeitosamente,

Sérgio Garcia Alves
Gerente de Políticas Públicas, Brasil

Raúl Echeberría
Diretor Executivo

_____

Associação Latino-americana de Internet (ALAI). https://alai.lat/

Assunto: Consulta Pública sobre o Regulamento de Comunicação de Incidente de Segurança com Dados Pessoais. Comentários e sugestões a artigos específicos da minuta de Regulamento.

CAPÍTULO II
DAS DEFINIÇÕES

- ***"Art. 3º Para efeitos deste Regulamento são adotadas as seguintes definições:"***

    - ***"I -*** I - ampla divulgação do incidente de segurança com dados pessoais 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, desde que a via eleita pelo controlador tenha se demonstrado ineficaz para fins de comunicação com os titulares afetados
        - **Comentário:** Conforme reconhecido pelo EDPB em seu "*Guidelines 9/2022 on personal data breach notification under GDPR*", o controlador se encontra em **melhor posição** para a escolha do canal mais apropriado para comunicar titulares a respeito do incidente. Ainda, a *"**ampla divulgação do incidente em meios de comunicação**"* não deve ser - em nenhum momento - confundida ou aproximada aos efeitos da aplicação da sanção administrativa de "***publicização da infração***" (art. 52, IV, LGPD), que, como se sabe, traz prejuízos de difícil mensuração à imagem e reputação da empresa frente ao mercado e consumidores.

          A conceituação de "*ampla divulgação do incidente em meios de comunicação*" deve se ater ao seu propósito de informar sobre o incidente e garantir ao titular a possibilidade de mitigação de danos, não devendo perpassar tal intuito e ter qualquer caráter e natureza sancionatória ou que possa expor indevida ou desproporcionalmente o agente regulado, causando danos à sua imagem, reputação, honra objetiva, já que não há possibilidade de ampla defesa do controlador.

    - ***"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;"***

- **Comentário:** A inclusão do conceito de autenticidade na minuta é prejudicial para a regulação da matéria, uma vez que foge da terminologia utilizada pela LGPD em seu art. 46, *caput*, que dispõe que "*Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito*". Da mesma forma, o termo também não consta do atual modelo de formulário de comunicação de incidente de segurança disponibilizado pela ANPD. Assim, a sua inclusão, por não haver paralelismo claro com as terminologias utilizadas pela LGPD e pela própria ANPD, gera insegurança jurídica. Para solucionar a questão, sugere-se uma leitura do conceito de incidente de segurança que seja o mais próximo possível da LGPD.

- A LGPD não define em seu art. 5º o termo "incidente de segurança". No entanto, em seu art. 46, a Lei apenas reproduz - em linguagem própria - a tríade comum da segurança da informação, qual seja, confidencialidade ("acessos não autorizados" e "comunicação"), integridade ("destruição" e "alteração") e disponibilidade ("perda"). Nos artigos seguintes, a Lei reiteradamente utiliza o termo "incidente de segurança", que logicamente remete às hipóteses de quebra de segurança dispostas no *caput* do art. 46, que inicia a Seção I (Da Segurança e do Sigilo de Dados) do Capítulo VII (Da Segurança e das Boas Práticas). Nesse sentido, conclui-se que a LGPD não inclui expressamente em sua definição de "incidente de segurança" a propriedade de autenticidade.

- Novamente, o próprio formulário de comunicação de incidente de segurança disponibilizado pela ANPD utiliza a tríade como parâmetro de comunicação. Em sua página 5, no tópico sobre os impactos do incidentes, a Autoridade questiona "*De que formas o incidente afetou os dados pessoais*". Sua resposta inclui as seguintes alternativas pré-disponibilizadas: **(i)** "*Confidencialidade*" - "*Houve acesso não autorizado aos dados, violando seu sigilo*"; **(ii)** "*Integridade*" - "*Houve alteração ou destruição de dados de maneira não autorizada ou acidental*"; e/ou **(iii)** "*Disponibilidade*" - "*Houve perda ou dificuldade de acesso aos dados por período significativo*".

- Portanto, em observância ao princípio da legalidade e visando maior segurança jurídica, sugerimos a supressão deste inciso, bem como a supressão do termo "autenticidade" nos demais artigos da minuta de Regulamento.

- ***"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;"***
  - **Comentário:** Sugere-se a exclusão, considerando que, na Lei Geral de Proteção de Dados Pessoais ("LGPD"), não foi feita uma escolha legislativa no sentido de categorizar dados pessoais de acordo com o contexto de sua utilização, entende-se que a presente minuta deve seguir o mesmo caminho. Nesse sentido, é importante destacar que a LGPD se restringe a diferenciar dados pessoais e dados pessoais sensíveis. Portanto, sugere-se a exclusão de tal definição, bem como de seus reflexos na minuta de resolução.

- ***"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;"***
  - **Comentário:** Em linha com a exclusão da hipótese de dados de autenticação em sistemas do art. 5º, IV deste regulamento, bem como da definição de autenticação do *caput deste artigo,* sugere-se a exclusão deste inciso, uma vez que o termo não será retomado em nenhuma outra oportunidade nesta minuta.

- ***"VII - dado financeiro: dado pessoal relacionado às transações financeiras do titular, inclusive para contratação de serviços e aquisição de produtos;"***
  - **Comentário:** Em linha com a exclusão da hipótese de dados financeiros do art. 5º, III deste regulamento, sugere-se a exclusão deste inciso, uma vez que o termo não será retomado em nenhuma outra oportunidade nesta minuta.
- ***"VIII - dado pessoal afetado: dado pessoal cuja confidencialidade, integridade, disponibilidade ou autenticidade tenha sido comprometida em um incidente de segurança;"***
  - **Comentário:** Em linha com a sugestão ao art. 3º, II, da minuta, sugerimos a exclusão da propriedade "autenticidade".

- ***"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;"***
  - **Comentário:** Sugere-se a supressão do inciso, tendo em vista que: (i) a LGPD se utiliza da terminologia "acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação"; e (ii) as propriedades confidencialidade, disponibilidade e integridade são princípios fundamentais da segurança da informação, já extensivamente definidas em normas internacionalmente consagradas e adotadas como boas práticas.

- ***"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;"***
  - **Comentário:** Sugere-se alteração no conceito de "*incidente de segurança com dados pessoais*" proposto pela ANPD na minuta, uma vez que ele está em desacordo com a LGPD, com o art. 3º, XII, da minuta e com a experiência internacional sobre o assunto. Expressões como "*qualquer evento adverso confirmado*" e "*propriedades de confidencialidade, integridade, disponibilidade e autenticidade*" dificultam a compreensão do objeto a ser definido e insere no texto da norma uma imprecisão injustificada, de modo que devem ser substituídas.

  - O termo "*incidente de segurança*" previsto na LGPD possui relação direta com os atos ilícitos que as medidas de segurança descritas no art. 46 visam conter, os quais deveriam ter sido utilizados e explorados na definição. Neste artigo, a Lei dispõe que as medidas de segurança, técnicas e administrativas visam proteger os dados pessoais de "*acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito*". Logo em seguida, no art. 48, a LGPD insere pela primeira vez o termo "*incidente de segurança*", a partir do qual define os critérios para a notificação à Autoridade. Em nenhum momento a LGPD utiliza os termos de "confidencialidade", "integridade" ou "disponibilidade" (propriedades da SI) de forma expressa e direta, assim como também não utiliza "evento adverso

confirmado" como tentativa de conceituação de incidente ou violação de segurança.

- Ademais, tanto o GDPR, quanto o *Personal Information Protection and Electronic Documents Act* do Canadá, não utilizam tais termos, mas apenas se valem de uma relação de causalidade entre a violação da segurança e o seu resultado:

- **Canadá (tradução livre)**[1]: "*violação das medidas de segurança significa* **[Consequência:]** *a perda, o acesso não autorizado ou a divulgação de informações pessoais* **[Causa:]** *resultantes de uma violação das medidas de segurança de uma organização referida na cláusula 4.7 do Anexo 1 ou de uma falha na implantação dessas medidas".*

- **GDPR (tradução livre)**[2]: "'*violação de dados pessoais significa* **[Causa:]** *uma violação de segurança que provoque,* **[Consequência:]** *de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso não autorizados, a dados pessoais transmitidos, armazenados ou sujeitos a qualquer outro tipo de tratamento*"

- Não há necessidade, portanto, de inserir novos termos cujo propósito seria apenas de elevação do grau de abstração da terminologia já empregada pela LGPD, que é suficiente para regular a matéria. Assim, sugerimos que a definição seja substituída por: "*incidente de segurança com dados pessoais: violação da segurança dos dados pessoais que resulte em acessos não autorizados ou situações acidentais ou ilícitas de destruição, perda, alteração ou comunicação.*"

CAPÍTULO III
DA COMUNICAÇÃO DE INCIDENTE DE SEGURANÇA
Seção I
Dos critérios para comunicação de incidentes de segurança

[1] "*breach of security safeguards means the loss of, unauthorized access to or unauthorized disclosure of personal information resulting from a breach of an organization's security safeguards that are referred to in clause 4.7 of Schedule 1 or from a failure to establish those safeguards. (atteinte aux mesures de sécurité).*"
[2] "*personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.*"

- ***"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."***
    - **Comentário:** É importante que a obrigação de notificar a ANPD seja desassociada da obrigação de notificar os titulares de dados pessoais. Tal dissociação já ocorre, por exemplo, dentro da estrutura normativa do GDPR, que em seus arts. 33 e 34 disciplina, respectivamente, **(i)** a notificação à autoridade em caso de incidente de segurança com dados pessoais que acarrete **risco** aos direitos e liberdade dos titulares; e **(ii)** a comunicação aos titulares nos casos de **alto risco**[3] aos direitos e liberdades dos titulares envolvidos.

    - Como se vê, não há gatilhos idênticos que justifiquem o envolvimento de ambos ao mesmo tempo e sob as mesmas condições e isso ocorre, naturalmente, porque o propósito da notificação para cada um é diferente. Até mesmo o EDPB, em suas Diretrizes 9/2022 sobre a notificação da violação de dados pessoais sob o GDPR, reafirma que "*o principal objetivo da notificação aos indivíduos é fornecer informação específica sobre as medidas que devem adotar para se protegerem (...) a comunicação ajudará as pessoas a adotarem medidas para se protegerem de quaisquer consequências negativas da violação*".

    - Para fins ilustrativos, o procedimento de notificação estabelecido pela SENACON em casos de recall é de que primeiro se notifica à SENACON sobre o início das investigações em caso de possibilidade de produtos ou serviços nocivos ou periculosos colocados no mercado e somente se concluída ou identificada a nocividade ou periculosidade é que surge o dever de informar os consumidores por meio de aviso de risco de acidente ao consumidor. Ainda que resguardadas as devidas diferenças regulatórias com a minuta de Regulamento, o que se busca destacar é que os gatilhos para notificar cada um (SENACON e consumidor) não são os mesmos (Portaria nº 618/2019). Se tal postura pode ser adotada em casos nos quais a apuração envolve possíveis riscos à própria vida dos consumidores, não há razão para

[3] Alguns exemplos trazidos pela ICO: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/data-protection-impact-assessments-dpias/examples-of-processing-likely-to-result-in-high-risk/

regulamentar a questão de forma diversa no que tange a incidentes de segurança com dados pessoais.

- Em relação à comunicação aos titulares de dados pessoais, em linha com o relatado no AIR (fl. 20), um dos principais benefícios/finalidades da comunicação é o de fornecer a informação para que possam adotar, caso queiram, as medidas assecuratórias cabíveis para reduzir o risco do incidente.

- Por conta disso, nem todo incidente reportável à ANPD deveria atrair - de forma obrigatória - a notificação ao titular. Essa notificação deveria ocorrer mediante gatilho da existência e identificação de que efetivamente existem medidas assecuratórias a serem implementadas pelo titular que podem ajudá-lo(a) na mitigação e redução dos riscos ou danos. Essa medida é recomendável, inclusive, para evitar a fadiga do titular em casos de múltiplas comunicações de incidentes, de modo que o contato entre controlador e titular atinja patamar eficiente e capaz de cumprir com a finalidade da comunicação.

- Além disso, sugere-se a inclusão de um parágrafo que explicite as hipóteses em que não é necessário comunicar um incidente de segurança à ANPD e aos titulares, como: **(i)** caso o controlador tenha implementado medidas adicionais suficientes para mitigação ou reversão dos riscos ou danos relevantes identificados, **(ii)** caso os dados afetados sejam anonimizados ou pseudoanonimizados, **(iii)** caso o incidente seja causado pelo próprio titular ou por terceiros, e **(iv)** caso os dados envolvidos no incidente sejam previamente públicos e o incidente não altere a disponibilidade e publicidade desses dados pessoais.

- ***"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:"***
  - **Comentário:** O art. 5º definiu que o "incidente de segurança com dados pessoais que pode acarretar risco ou dano relevante aos titulares" é aquele que "**tiver potencial**" de "afetar significativamente interesses e direitos fundamentais dos titulares", além de envolver um

dos critérios descritos nos incisos (dados sensíveis; dados de crianças, de adolescentes ou de idosos; dados financeiros; dados de autenticação em sistemas; ou dados em larga escala). Contudo, verifica-se que tanto o termo "tiver potencial" quanto a falta de concretude no termo "afetar significativamente interesses e direitos dos titulares" implicam em ampla margem para o que pode ser considerado incidente de segurança a ser comunicado para a ANPD.

- Considerando que a mera afetação de interesses e direitos fundamentais dos titulares já se revela uma situação excessivamente ampla, com muito mais razão o é a sua potencialidade. A atual definição, se aprovada, abrangerá uma infinidade de casos e proporcionará um esvaziamento da própria funcionalidade do instituto da notificação, razão pela qual se faz necessária a sua modificação. Assim, sugerimos a retirada do termo "*tiver potencial*" dentro de "tiver potencial de afetar significativamente interesses e direitos fundamentais".

- ***"V - dados em larga escala."***
  - **Comentário:** Ainda que o § 2º deste artigo defina incidentes de segurança com dados pessoais em larga escala como aqueles que "*abrangem um número significativo de titulares, considerando, ainda, o volume de dados envolvidos e a extensão geográfica de localização dos titulares*", essa definição ainda é dotada de grande subjetividade. Tais hipóteses nem sempre são suficientes para configurar situações que por si só acarretem risco ou dano relevante aos titulares, dado que é possível que um grande número de atividades de tratamento (algumas, inclusive, corriqueiras e de baixa complexidade) venham a ser encaixadas neste conceito. É crucial que a ANPD determine, em regulamento próprio, seu entendimento sobre critérios mais objetivos acerca do que caracteriza "larga escala" no contexto de operações de tratamento de dados pessoais, não se afigurando suficiente para esta finalidade o disposto no § 2º. Dessa forma, sugere-se a remoção desse dispositivo.

- ***"§ 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"

- **Comentário:** A ausência de delimitação do conceito de serviço torna o dispositivo altamente genérico e impreciso. Seria impossível sustentar que há violação aos interesses e direitos fundamentais a partir da limitação de utilização de qualquer tipo de serviço, uma vez que há serviços que são mais ou menos essenciais à vida humana, de tal forma que é possível haver ocasiões em que seus impactos nos interesses ou direitos fundamentais são muito baixos ou mesmo inexistentes. Por exemplo, considera-se que serviços de saúde e educação possuem alto impacto nos interesses e direitos fundamentais, enquanto serviços de entretenimento teriam um potencial menor de afetá-los. Sugere-se, portanto, que haja a inclusão do adjetivo "*essencial*" ao lado de serviço, para que esta categoria seja delimitada posteriormente pela ANPD.

- ***"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."***
  - **Comentário:** A menção do dispositivo a "*danos materiais ou morais aos titulares*" como um dos critérios para considerar incidentes com potencial de afetar significativamente interesses e direitos fundamentais dos titulares traz para o controlador o exercício de antever as situações que configurariam esses danos materiais ou morais. Em outras palavras, o artigo atribui ao controlador a tarefa de julgar e antever o que é objeto de ampla discussão e provas até mesmo perante o Poder Judiciário, o que é indevido.

  - Ademais, é imperioso notar que a ideia de "possibilidade de danos de ordem material ou moral aos titulares", mencionada no referido voto, não se confunde com a ideia de dano presumido. Isto é, a própria linha de raciocínio da Autoridade é no sentido de que dever-se-ia levar em consideração a possibilidade de que danos materiais ou morais sejam sofridos pelos titulares. Embora questionável, não há dúvidas de que este foi o norte da ANPD, não sendo possível confundir o conceito de "risco de dano" com o de "dano presumido". Ao tratar dos critérios que devem ser considerados na avaliação das consequências do incidente, afirma o Diretor Relator que: "(...) *para este Regulamento importa a avaliação das consequências, isto é, dos*

impactos advindos de incidentes de segurança envolvendo dados pessoais, à esfera de direitos e interesses dos titulares (...)". Naturalmente, a melhor avaliação das consequências é aquela calcada não na presunção de um dano, mas sim na sua concretização e comprovação.

- Neste sentido, de acordo com o entendimento do STJ no bojo do AResp nº 2.130.619/SP, em que pese ser uma falha indesejável, o vazamento de dados pessoais não é capaz de, por si só, gerar dano moral indenizável, de modo que é indispensável a comprovação, por parte do titular, de que tal exposição de suas informações lhe causou dano.

- Conforme proposto acima com relação ao art. 5º, *caput*, da minuta, para que se considere "*que um incidente de segurança com dados pessoais pode acarretar risco ou dano relevante aos titulares quando afetar significativamente interesses e direitos fundamentais dos titulares*", é imprescindível que se esteja diante de um dano que possa ser efetivamente concretizado e comprovado, jamais um dano presumido.

- Assim, caso a ANPD entenda que a possibilidade de se ocasionar danos materiais ou morais aos titulares engloba não apenas os danos efetivamente concretizados e comprovados, mas também os danos presumidos (isto é, que prescindem de comprovação por parte dos titulares), este entendimento pode ser rechaçado não apenas a partir da leitura do voto do Diretor Relator, como também a partir do recente posicionamento do STJ acerca da imprescindibilidade de comprovação do dano efetivamente sofrido pelo titular para que este faça jus a uma indenização pelo vazamento de seus dados.

Seção II
Da comunicação do incidente 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:"***

- **Comentário:** O prazo razoável para identificação do incidente e comunicação à Autoridade revela-se um dos temas mais sensíveis da minuta de Regulamento. Nessa linha, de acordo com pesquisa divulgada pela IBM Security – Cost of a Data Breach Report 2022, o tempo médio global para identificação e contenção de incidentes é de cerca de 277 dias.

- Assim, conclui-se que o prazo de 3 (três) dias úteis estipulado na minuta é desproporcional à função atrelada ao controlador de investigação de um incidente, proposição de medidas de reversão ou mitigação dos riscos ou danos relevantes e direcionamento de times e recursos internos e externos adequados para solução do problema. Esse ônus regulatório pode acarretar, inclusive, o desvio da atenção do controlador para a mitigação dos riscos e danos relevantes a pretexto de notificar a Autoridade.

- Ademais, consequência desse prazo tão curto será um número exacerbado de comunicações à ANPD, inclusive desperdiçando-se o tempo e recursos administrativos da ANPD com um efeito de fadiga das comunicações.

- Nesse sentido, destaca-se que, ao publicar orientações sobre notificações de incidentes de segurança com dados pessoais, a legislação Australiana (Privacy Act 1988), na seção 26WH, estabeleceu o prazo de 30 (trinta) dias para a finalização de uma avaliação que determine se o incidente de segurança com dados pessoais tem a probabilidade de resultar danos graves aos indivíduos.

- O prazo de 30 (trinta) dias úteis se revela uma alternativa operacionalmente mais viável para que os controladores - sobretudo em casos em que há compartilhamento de dados pessoais com outros agentes de tratamento envolvidos (operadores e sub operadores) - possam avaliar internamente os detalhes do incidente, a fim de que a notificação possa ser feita nos moldes requeridos pela ANPD.

- Sendo assim, sugere-se que o dispositivo seja reformulado para indicar que os agentes de tratamento terão: **(i)** 30 (trinta) dias úteis para notificar a ANPD sobre a ocorrência de incidente de segurança com dados pessoais que possa acarretar risco ou dano relevante aos

titulares afetados; e **(ii)** que tal prazo deve ter sua contagem iniciada a partir da constatação de que o incidente de segurança com dados pessoais pode gerar esse risco ou dano, ou do momento em que se tenha as informações mínimas necessárias para preenchimento do formulário de comunicação de incidente de segurança com dados pessoais, jamais do mero conhecimento do incidente de segurança.

- ***"II - o número de titulares afetados, discriminando, quando aplicável, o número de crianças, de adolescentes ou de idosos;"***
  - **Comentário:** Em alguns casos, não é operacionalmente possível estipular a quantidade exata do número de titulares afetados, nem mesmo de crianças, adolescentes ou idosos envolvidos no vazamento, devendo esta análise ser informada pelo controlador somente quando técnica e administrativamente possível. Por fim, a minuta da norma trouxe uma categoria especial para os dados de idosos que não encontra fundamento na LGPD, pelo que sugerimos a supressão de sua menção.

- ***"XI - a declaração de que foi realizada a comunicação aos titulares, nos termos do art. 10 deste Regulamento;"***
  - **Comentário:** A menção ao art. 10 deste Regulamento está equivocada, já que é o artigo inaugural do Capítulo IV que dispõe sobre o "Registro de Incidentes de Segurança com Dados Pessoais". A menção correta para se referir à comunicação do incidente ao titular de dados pessoais seria o art. 9º deste Regulamento.

  - Não obstante, entende-se que a inclusão deste inciso estabelece a comunicação de incidente de segurança aos titulares como pressuposto para a comunicação do incidente de segurança com dados pessoais à ANPD. Ou seja, ao dispor que a comunicação aos titulares deve compor o conjunto de informações a ser entregue junto com a comunicação à ANPD, pressupõe que os titulares sejam comunicados não concomitantemente ou posteriormente à ANPD, mas antes dela. Defende-se, portanto, que este inciso seja retirado (i) já que não encontra guarida no art. 48, §1º da LGPD; e (ii) para dar concretude à possibilidade de notificação à ANPD e aos titulares em prazos distintos.

- Caso se entenda pela manutenção do dispositivo, defendemos a inclusão da expressão “se cabível”.

- ***“XIII - o total de titulares cujos dados são tratados pela organização e na atividade de tratamento afetada pelo incidente.”***
  - **Comentário:** A informação a respeito do “*total de titulares cujos dados são tratados pela organização*” não está associada ao interesse atrelado ao instituto da comunicação do incidente de segurança à ANPD. Vale observar que o inciso II do §1º do art. 48 da LGPD dispõe que a comunicação deverá mencionar as informações apenas sobre “os titulares envolvidos”. Logo, sugere-se a supressão do inciso.

- ***“§ 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.”***
  - **Comentário:** A possibilidade de complementação das informações revela-se uma alternativa necessária para que os controladores - sobretudo em casos em que há o compartilhamento de dados pessoais com demais partes envolvidas (operadores e sub operadores) - possam avaliar internamente o nível de risco do incidente e filtrar o incidente para que a comunicação seja a mais completa possível, situações que são do interesse da própria ANPD.

  - Veja-se que esta hipótese é, inclusive, admitida por outras agências, como a ANAC, por exemplo, ao dispor na Instrução Normativa nº 174/2021: “*Art. 17-A. Se as informações existentes na manifestação forem insuficientes para o seu tratamento, poderá ser solicitada a complementação de informações ao usuário. § 1º O prazo para o atendimento do pedido de complementação de informações pelo usuário é de 20 (vinte) dias contados da data do seu recebimento, nos termos do § 2º do art. 18 do Decreto nº 9.492, de 2018*”.

  - Nesse sentido, a minuta peca em **(i)** estipular o início da contagem do prazo de vinte dias úteis como sendo a partir do “conhecimento do incidente”; e **(ii)** ao prever o termo “excepcionalmente”. Sugere-se que o prazo se inicie a partir do protocolo da comunicação original, bem como a exclusão do termo que confere regime de excepcionalidade ao artigo.

- ***"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."***
    - **Comentário:** A solicitação de tramitação de processos ou documentos e informações em sigilo vem sendo fundamentada em diversas legislações:

    - **(i)** Lei nº 9.279/1996, Art. 206. *Na hipótese de serem reveladas, em juízo, para a defesa dos interesses de qualquer das partes, informações que se caracterizem como confidenciais, sejam segredo de indústria ou de comércio, deverá o juiz determinar que o processo prossiga em segredo de justiça, vedado o uso de tais informações também à outra parte para outras finalidades.*

    - **(ii)** CPC, Art. 189*. Os atos processuais são públicos, todavia tramitam em segredo de justiça os processos: I - em que o exija o interesse público ou social; II - que versem sobre casamento, separação de corpos, divórcio, separação, união estável, filiação, alimentos e guarda de crianças e adolescentes; III - em que constem dados protegidos pelo direito constitucional à intimidade; IV - que versem sobre arbitragem, inclusive sobre cumprimento de carta arbitral, desde que a confidencialidade estipulada na arbitragem seja comprovada perante o juízo.*

    - (iii) *LAI,* Art. 6º *Cabe aos órgãos e entidades do poder público, observadas as normas e procedimentos específicos aplicáveis, assegurar a: I - gestão transparente da informação, propiciando amplo acesso a ela e sua divulgação; II - proteção da informação, garantindo-se sua disponibilidade, autenticidade e integridade; e III - proteção da informação sigilosa e da informação pessoal, observada a sua disponibilidade, autenticidade, integridade e eventual restrição de acesso.*
      Art. 7º § 2º Quando não for autorizado acesso integral à informação por ser ela parcialmente sigilosa, é assegurado o acesso à parte não sigilosa por meio de certidão, extrato ou cópia com ocultação da parte sob sigilo.

Art. 21. *Não poderá ser negado acesso à informação necessária à tutela judicial ou administrativa de direitos fundamentais. Parágrafo único. As informações ou documentos que versem sobre condutas que impliquem violação dos direitos humanos praticada por agentes públicos ou a mando de autoridades públicas não poderão ser objeto de restrição de acesso. Art. 22. O disposto nesta Lei não exclui as demais hipóteses legais de sigilo e de segredo de justiça nem as hipóteses de segredo industrial decorrentes da exploração direta de atividade econômica pelo Estado ou por pessoa física ou entidade privada que tenha qualquer vínculo com o poder público.*

- Assim, sugere-se que, havendo necessidade e fundamento para a alegação de sigilo de informações protegidas por lei, a exemplo das relativas à sua atividade empresarial cuja divulgação possa representar violação de segredo comercial ou industrial, haja a possibilidade de se determinar a tramitação sigilosa durante todo o processo de comunicação de incidentes. A adição dos incisos e parágrafos a seguir buscam contemplar essas hipóteses:
  "*§ 1º - Sempre que cabível, a Autoridade poderá, de ofício ou a requerimento do controlador, decretar a tramitação em sigilo de todo o processo de comunicação quando:*
  I - envolva exposição de dados protegidos pelo direito constitucional à intimidade, dados sensíveis ou dados de crianças ou adolescentes;
  II - garantir a proteção do segredo de indústria ou de comércio, bem como para preservar o uso de tais informações por terceiros ou concorrentes; e
  III - a tramitação pública do processo puder prejudicar a condução das investigações do incidente pelo controlador ou pela ANPD.
  §2º - O disposto no parágrafo primeiro deste artigo não exclui a apreciação pela Autoridade de pedido de tramitação sigilosa fundamentado em demais hipóteses legais de sigilo."

- ***"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."***

- **Comentário**: O artigo utiliza termos que dão ampla discricionariedade à ANPD, como "*a qualquer tempo*" e "*estabelecendo prazo para envio das informações*".

- Diante disso, recomenda-se que a solicitação de informações adicionais por parte da Autoridade ocorra até a conclusão do processo de comunicação de incidente com dados pessoais, com o trânsito em julgado da decisão administrativa. Além disso, para assegurar que a ANPD estabeleça prazos factíveis para que o controlador forneça informações adicionais, recomenda-se que esse prazo respeite o mínimo de 20 dias úteis (seguindo o paralelismo com os demais prazos da minuta) ou de 15 dias úteis, caso o paralelismo ocorra com os artigos do CPC**.**

- Em adição, é importante que o dispositivo reflita a proteção aos segredos comercial e industrial, sendo esta uma das atribuições previstas pela LGPD (art. 55-J II) à ANPD, que determina competir à ANPD zelar pelos segredos comercial e industrial.

Seção III
Da comunicação do 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:"***
    - **Comentário:** O prazo de apenas 3 (três) dias úteis para a notificação dos titulares dos dados pessoais é exíguo, principalmente considerando-se que muitas vezes sequer será possível identificar, nesse prazo, quais titulares foram efetivamente afetados pelo incidente.

    - É necessário considerar que algumas situações demandam maior prazo para apuração do incidente antes de se notificar o titular, em especial em casos que eventualmente demandem pareceres técnicos mais aprofundados para delimitar os eventos e o alcance do incidente,

bem como para que se conclua a respeito de riscos ou danos relevantes que justifiquem sua comunicação ao titular.

- Além disso, conforme dito, algumas situações mais simples não deveriam ensejar a necessidade de notificação dos titulares, principalmente se não houver alto risco ou medidas assecuratórias a serem tomadas por estes, bastando medidas internas da empresa para eliminar ou mitigar drasticamente os riscos e danos. Ademais, a comunicação prematura e indevida ao titular pode, desnecessariamente, gerar pânico, ainda que não haja riscos aos titulares, o que não atende aos melhores interesses dos titulares e nem mesmo da ANPD.

- Ademais, a notificação em curto espaço de tempo torna o controlador vulnerável e suscetível aos efeitos prejudiciais que a comunicação precipitada pode ocasionar à sua atividade (sejam prejuízos de imagem, reputacionais, boicotes, investigação de outras autoridades competentes etc.).

- Portanto, sugerimos 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, ou seja, 60 (sessenta) dias. Ademais, 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.

- ***"§ 1º A comunicação do incidente aos titulares de dados deverá atender aos seguintes critérios:***
  II - ocorrer de forma direta e individualizada, caso seja possível identificá-los."
  - **Comentário:** Deve-se privilegiar o meio e forma de comunicação eleitos pelo controlador, porquanto é quem tem mais conhecimento do contexto e pode entender qual a melhor maneira de se comunicar, eficazmente, com os titulares afetados. Nesse sentido, destaca-se que o *Working Party 29 (Guidelines on Personal data breach notification under Regulation 2016/679)* pontua que os controladores estão na melhor posição para determinar o canal mais adequado para

comunicar os titulares. Em complemento, no mesmo documento, indica-se que os controladores devem escolher o meio de comunicação que maximize as chances de que as informações necessárias cheguem àqueles afetados pelo ocorrido. Sendo assim, sugere-se que o dispositivo em questão seja reformulado para "*ocorrer da maneira mais eficaz para alcançar os titulares afetados, podendo ser de maneira generalizada ou de forma direta e individualizada, a critério do controlador.*"

- ***"§ 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."***
  - **Comentário:** Como comentado em relação ao inciso II do §1º do presente artigo, entende-se que o controlador é o melhor agente para determinar qual o meio mais adequado para comunicar os titulares afetados visando maximizar o alcance da notificação. Sendo assim, é preciso que se reformule o presente dispositivo, visto que a redação atual implica a preferência de uma comunicação direta e individualizada.

  - Em outro ponto, sugere-se a redução do período mínimo de 6 (seis) meses contido na norma deste parágrafo para 60 (sessenta) dias, um período de tempo razoável para que os titulares possam tomar as providências que entenderem necessárias de forma a salvaguardar seus direitos. O prazo mínimo de seis meses pode, inclusive, ser excessivo quando se relaciona com agentes de pequeno porte que tratam poucos dados ou até mesmo com qualquer agente de tratamento que detém facilidade de contato com os titulares, ou cuja comunicação tenha alcançado seu propósito. Assim, entende-se que a sugestão apresentada se faz necessária para que a comunicação pública do incidente de segurança não se confunda com ou tenha potencial mais gravoso do que a sanção de publicização prevista nos arts. 20 e 21 da Resolução CD/ANPD nº 4/2023, que sequer possui prazos pré-estabelecidos, conforme art. 20, §2º: "*A sanção de*

publicização deverá indicar o teor, o meio, a duração e o prazo para o seu cumprimento"

- ***"§ 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."***
  - **Comentário:** Entendemos que a comunicação aos titulares deve se dar após a notificação da ANPD e pelo controlador que tiver dado causa ao incidente de segurança com dados pessoais, logo, sugerimos a alteração do dispositivo.

  - Sugestão de texto: § 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~~, se necessário, nos termos do *caput* do art. 9º, que comunique o incidente de segurança com dados pessoais 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."***
  - ***Comentário: Na linha da regulação responsiva, seria importante a ANPD considerar sempre como boa prática medidas proativas adotadas pelos agentes de tratamento de dados que atendam ao previsto na LGPD e mitiguem danos a titulares em caso de eventual incidente de segurança com dados pessoais. Desta forma, tal consideração não precisaria ficar sujeita à discricionariedade administrativa, mas, sim ser, concedida como um direito do agente de tratamento, representando um estímulo ao desenvolvimento dessas práticas.***

  - ***Ademais, o Regulamento de Dosimetria e Aplicação de Sanções Administrativas prevê em seu artigo 13, II, a redução da sanção pecuniária em 20% (vinte por cento) nos casos de implementação de política de boas práticas e de governança ou de adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar os danos aos titulares. Neste mesmo caso, a comunicação ao titular de recomendações e as ações educativas, para fins deste***

Regulamento também devem ser consideradas boas práticas e atenuantes a serem consideradas no processo administrativo sancionador.

- ***Sugestão de texto: § 5º Poderá ser Será 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.***

CAPÍTULO IV
DO REGISTRO DE INCIDENTES 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."***
  - **Comentário:** Segundo as obrigações relacionadas ao *Personal Information Protection and Electronic Documents Act* (PIPEDA), do Canadá, na página "*What you need to know about mandatory reporting of breaches of security safeguards*": "*A lei exige que você mantenha registros de violação de todas as violações de salvaguardas de segurança por dois anos. Você pode ter outros requisitos legais que podem exigir que você os mantenha por mais tempo.*" Esse prazo se mostra mais razoável do que o prazo mínimo de 5 (cinco) anos proposto no Regulamento, sem prejuízo da possibilidade de se manter os registros do incidente por prazo superior, por opção do controlador, caso sejam aplicáveis outras bases legais previstas na LGPD que justifiquem a retenção por tempo maior.

CAPÍTULO V
DO PROCESSO DE COMUNICAÇÃO DE INCIDENTE DE SEGURANÇA COM DADOS PESSOAIS
Seção I
Das disposições gerais

- ***"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."

- **Comentário:** É importante considerar que os incidentes de segurança com dados pessoais são inseridos num contexto e são dotados de particularidades incompatíveis com uma análise feita de forma agregada. Além disso, considerando que a LGPD estabelece uma abordagem baseada em risco e uma regulação responsiva, análises agregadas e providências padronizadas servem como um desestímulo aos controladores e vão de encontro com o Regulamento de Dosimetria e Aplicação de Sanções Administrativas (Resolução CD/ANPD 4/2023). Desta feita, sugere-se a exclusão do presente artigo e de seu parágrafo único.

- Tendo em vista a sugestão de supressão do *caput* do artigo 13, recomenda-se o ajuste do presente parágrafo nos seguintes termos:

- Artigo 13. Os processos ~~referidos no caput~~ de comunicação de incidente de segurança com dados pessoais, de que trata este Regulamento, 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."***

  - **Comentário:** Sugere-se a retirada do trecho "*sem prévia manifestação do controlador*", de modo que o controlador possa apresentar sua manifestação a respeito das determinações da ANPD para a adoção de medidas preventivas necessárias para salvaguardar direitos dos titulares ou para reverter ou mitigar os efeitos do incidente, considerando, principalmente, que o controlador tem conhecimento sobre seu próprio ramo de negócio e, portanto, domínio da técnica (o que confere maior qualidade à tomada de decisão). Também

sugere-se a possibilidade de requerer efeito suspensivo à determinação da ANPD, dado que o controlador está sujeito - em caso de descumprimento - à 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).

- Vale mencionar que as medidas preventivas necessárias para salvaguardar direitos dos titulares ou para reverter ou mitigar os efeitos do incidente, previstas no artigo 14 da minuta e no art. 48, § 2º, II da LGPD, não se confundem com as medidas corretivas previstas no art. 2º, V, da Resolução CD/ANPD nº 4/2023, que dispõe: "*medidas determinadas pela ANPD com a finalidade de corrigir a infração e reconduzir o infrator à plena conformidade à LGPD e aos regulamentos expedidos pela ANPD, devendo ser aplicadas conjuntamente com a sanção de advertência*".

- Ainda, as medidas preventivas dispostas no art. 31 do Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador incluem: (a) divulgação de informações; (b) aviso; (c) solicitação de regularização ou informe; e (d) plano de conformidade. Outras medidas preventivas podem ser determinadas desde que com a finalidade de recondução do agente de tratamento à conformidade ou para evitar ou remediar situações de risco ou dano relevante (arts. 30 e 31, § 1º do Regulamento).

- Tal confusão não deve ocorrer em razão das medidas preventivas serem aplicadas após o trâmite do processo administrativo sancionador, uma vez instaurado e garantido o contraditório e ampla defesa. No processo de comunicação de incidente, por sua vez, o objetivo não é apurar a infração em si (visto que a partir de indícios de infração instaura-se o processo administrativo sancionador), mas tão somente salvaguardar o titular afetado no incidente reportado ou apurado.

Seção II

Do procedimento de apuração de incidente de segurança

- ***"Art. 16, §1º A ANPD poderá fixar multa diária para assegurar o cumprimento da determinação prevista no caput.***
    - **Comentário:** A multa diária, em leitura conjunta desta minuta de Regulamento e do Regulamento de Dosimetria e Aplicação de Sanções Administrativas, poderá ser aplicada para assegurar o cumprimento, em prazo certo, de uma sanção não pecuniária ou de uma determinação estabelecida pela ANPD. Contudo, devem ser observadas as hipóteses em que essa multa cominatória se aplicará, conforme disposto no § 3º do art. 16 do Regulamento de Dosimetria e Aplicação de Sanções Administrativos, que dispõe *"A sanção de multa diária poderá ser aplicada na hipótese do caput deste artigo ou quando o infrator: I - após notificado do cometimento de irregularidades que tenham sido praticadas, deixar de saná-las no prazo assinalado; II - praticar obstrução à atividade de fiscalização, desde que a aplicação da multa diária seja necessária para desobstrui-la; ou III - praticar infração permanente não cessada até a decisão"*

    - § 1º A ANPD poderá fixar multa diária para assegurar o cumprimento da determinação prevista no caput, após ter notificado o controlador do cometimento de irregularidades que tenham sido praticadas e este deixar, de forma injustificada, de saná-las no prazo assinalado.

-

Seção III

Do procedimento de comunicação de incidente de segurança

-
- ***"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."***
    - **Comentário:** Apesar do poder conferido à ANPD pela LGPD de realizar auditorias no âmbito da atividade de fiscalização (art. 55-J, XVI), recomenda-se que seu procedimento seja desenhado de forma mais restrita, no âmbito do processo de comunicação do incidente de segurança com dados pessoais, e apenas quando absolutamente necessárias para subsidiar as determinações da ANPD sobre a adoção

de providências e medidas para reverter ou mitigar os efeitos do incidente para salvaguardar direitos dos titulares (em coerência com o disposto nos arts. 14 e 19 da minuta).

- Busca-se, com isso, afastar o procedimento de comunicação da espécie e natureza de um procedimento preparatório em que se busca a coleta de evidências para juntadas dos indícios da prática de infração para que se justifique a instauração do processo administrativo sancionador.

- Ademais, devem ser preservados, em quaisquer hipóteses, os segredos comerciais e industriais, o sigilo profissional do auditor e a possibilidade de o controlador opor-se - a qualquer momento - ao auditor nomeado.

- Deve-se preservar também a possibilidade de manifestação do controlador a respeito do despacho determinando a auditoria, de modo que este possa alegar incongruência entre o escopo da auditoria e o incidente reportado, hipóteses de segredo comercial ou industrial, dentre outros questionamentos que se façam pertinentes a partir do caso concreto.

- ***"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 incidente em meios de comunicação; ou"***
    - **Comentário:** Sugerimos alteração do dispositivo para que conste expressamente: "*ampla divulgação do incidente de segurança com dados pessoais em meios de comunicação, desde que a via eleita pelo controlador tenha se demonstrado ineficaz para fins de comunicação com os titulares afetados.*"

  - ***"§ 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."***
    - **Comentário:** A *"ampla divulgação do incidente em meios de comunicação"* não deve ser - em nenhum momento - confundida ou

aproximada aos efeitos da aplicação da sanção administrativa de "*publicização da infração*" (art. 52, IV, LGPD).

- Nesse sentido, a divulgação, pela ANPD, em sua página na Internet, de informações relativas a incidentes de segurança com dados pessoais deve ocorrer somente com a finalidade de instruir os titulares de dados pessoais, sem, contudo, expor o agente regulado que tenha comunicado o incidente à ANPD e o tipo de incidente sofrido. Tal medida é importante, inclusive, para que não se crie um ambiente de desincentivo às notificações, visto que o controlador estaria sujeito a um dano reputacional sem que tenha passado por um processo administrativo sancionador, com direito à ampla defesa e contraditório.

- ***"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."***
  - **Comentário:** Novamente, a *"ampla divulgação do incidente em meios de comunicação"* não deve ser - em nenhum momento - confundida ou aproximada aos efeitos da aplicação da sanção administrativa de "*publicização da infração*" (art. 52, IV, LGPD).

  - A conceituação de "*ampla divulgação do incidente em meios de comunicação*" deve se ater ao seu propósito de informar ao titular os incidentes em que este pode implementar medidas assecuratórias, não devendo perpassar tal intuito e ter qualquer caráter sancionatório ou que possa expor indevida ou desproporcionalmente o agente regulado, já que não há possibilidade de ampla defesa do controlador. Também deve-se privilegiar a lógica de que o controlador é o melhor posicionado para a escolha da via de comunicação com o titular, sendo possível a atuação da ANPD tão somente nos casos em que a via eleita pelo controlador não se mostre suficiente.

- ***"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."

- **Comentário:** para que haja uma leitura deste artigo alinhada com o conceito de medidas de segurança (previsto no art. 3º, XII desta minuta e na LGPD, art. 46), recomenda-se a eliminação dos termos "confidencialidade", "integridade", "disponibilidade" e "autenticidade". Entende-se que o termo *"medidas para reverter ou mitigar os efeitos do incidente"* deve vir associado a "*acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação*".
- Ademais, entendemos que, embora a ANPD – enquanto autoridade competente – possa determinar ao controlador a adoção de determinadas medidas, é importante que tais imposições levem em consideração as medidas mitigatórias tomadas e/ou já em curso, bem como o plano de resposta a incidentes e eventuais ações planejadas pelo controlador. Caso contrário, uma atuação arbitrária e descontextualizada por parte da ANPD pode acabar por prejudicar as ações de contenção, investigação e mitigação de efeitos do incidente. Por tal razão, entendemos que o dispositivo deve ser alterado para inserir a possibilidade de que o controlador se manifeste
- Sugestão de texto: Art. 21. Na determinação pela ANPD das medidas para reverter ou mitigar os efeitos do incidente de segurança com dados pessoais, serão consideradas aquelas que possam ~~garantir a confidencialidade, a integridade, a disponibilidade e a autenticidade dos dados pessoais afetados~~, proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração ou comunicação, bem como minimizar os efeitos decorrentes do incidente de segurança com dados pessoais para os titulares de dados, garantido o direito de manifestação do controlador.

- ***"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."***
  - **Comentário:** A instauração de processo administrativo sancionador e eventual aplicação de sanções administrativas devem observar as leis sobre processo administrativo federal com peculiaridades trazidas pelas Resoluções CD/ANPD nºs 01/2021 e 4/2023, respectivamente, devendo ser sempre garantido ao controlador o exercício do direito ao

contraditório e à ampla defesa. Nesse sentido, é fundamental a verificação, pela ANPD, da possibilidade técnica de o controlador adotar as medidas que pretender determinar visando a reversão ou mitigação dos efeitos do incidente, de modo a não penalizar o controlador injustamente com a atividade repressiva. Prestigiando a regulação responsiva, os princípios da eficiência e da razoabilidade, a ANPD, ao entender o contexto do controlador e priorizar medidas que ele possa realizar, alcançará, da forma mais eficaz possível, os objetivos principais do processo de comunicação de incidente de segurança com dados pessoais, quais sejam, o de proteger direito dos titulares e mitigar ou reverter o risco de dano aos titulares afetados. Deste modo, entende-se a necessidade de alteração do *caput* do dispositivo para que tais preocupações sejam endereçadas.

- Não obstante, na hipótese de a ANPD entender que o processo administrativo sancionador deverá realmente ser instaurado, revela-se extremamente necessária a consideração de dispositivo legal que a ANPD deixou de regulamentar na minuta desta Resolução. Referimo-nos ao §7º do artigo 52 da LGPD que determina: *"Os vazamentos individuais ou os acessos não autorizados de que trata o caput do art. 46 desta Lei poderão ser objeto de conciliação direta entre controlador e titular e, caso não haja acordo, o controlador estará sujeito à aplicação das penalidades de que trata este artigo."* Nota-se que a LGPD criou uma condição suspensiva à aplicação de sanções administrativas pela ANPD quando ocorrer vazamento individual ou acesso não autorizado de dados pessoais. Ou seja, quando houver um processo administrativo sancionador já instaurado contra um controlador, em virtude de vazamento individual, ou em caso de acessos não autorizados, e este estiver em negociação de um acordo com o titular afetado, a ANPD somente poderá aplicar sanção administrativa se o acordo entre eles não for realizado. A LGPD criou uma hipótese de suspensão do processo administrativo sancionador antes da determinação de sanção administrativa ao estimular o acordo direto entre o controlador e o titular afetado. Deste modo, sugere-se a inserção de um parágrafo neste dispositivo para regulamentar o incentivo à conciliação direta determinado pela LGPD e a não aplicação da sanção administrativa quando houver acordo direito do controlador e titular.

- Sugestão de texto: Art. 23. A ANPD poderá instaurar processo administrativo sancionador caso o controlador, dentro de suas competências técnicas, 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, observadas as Resoluções CD/ANPD nºs 01/2021 e 4/2023.

- Parágrafo único: Havendo instauração de processo administrativo sancionador em caso de vazamentos individuais ou acessos não autorizados e, existindo negociação direta visando a realização de acordo entre o controlador e o titular afetado, a ANPD somente aplicará sanção administrativa se, instado a se manifestar, o controlador informar que não foi possível a conciliação direta.

- ***"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:"***
    - **Comentário:** Sugerimos a inclusão de outras hipóteses de extinção do processo de comunicação de incidente de segurança com dados pessoais ao final do procedimento de comunicação de incidente, como: **(i)** caso o controlador tenha implementado medidas adicionais suficientes para mitigação ou reversão dos riscos ou danos relevantes identificados, **(ii)** caso os dados afetados sejam anonimizados ou pseudoanonimizados, **(iii)** caso o incidente seja causado pelo próprio titular ou por terceiros, e **(iv)** caso os dados envolvidos no incidente sejam previamente públicos e o incidente não altere a disponibilidade e publicidade desses dados pessoais.
  - ***Sugestão de inclusão § 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.

CAPÍTULO VI
DAS DISPOSIÇÕES FINAIS