ANPD Autoridade Nacional de Proteção de Dados

CIPL AT 20 — SHAPING DATA POLICY FOR TOMORROW
HUNTON ANDREWS KURTH

MODELO PARA ENVIO DE CONTRIBUIÇÕES REFERENTE À TOMADA DE SUBSÍDIOS Nº 2/2021

NOME DA INSTITUIÇÃO/PESSOA FÍSICA: Centre for Information Policy Leadership (CIPL)

CPF/CNPJ: N/A

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

INTRODUÇÃO

As questões a seguir buscam direcionar a tomada de subsídios da nova regulamentação aplicável à comunicação a ser feita à ANPD e ao titular de dados sobre a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Muito embora a lei estabeleça critérios mínimos, é preciso que a ANPD regulamente alguns itens, como prazo, e defina o formulário e a melhor forma de encaminhamento das informações, nos termos do art. 48 e seguintes da Lei nº 13.079 de 14 de agosto de 2018 e do item 3 da Agenda Regulatória 2021-2022 da ANPD.

São apresentadas questões como critérios para avaliação de risco ou dano relevante pela ANPD; distinção entre risco ou dano; considerações que devem ser feitas na avaliação de risco ou dano; informações que os controladores devem apresentar à ANPD e aos titulares; definição do prazo razoável para informar tanto a ANPD quanto os titulares; e possíveis exceções quanto à obrigatoriedade de informar a ANPD e os titulares, dentre outros abaixo elencados.

Outros temas considerados relevantes para a análise de impacto regulatório da regulamentação podem ser inseridos na tabela.

SOBRE O CIPL

O Centre for Information Policy Leadership (CIPL) recebe com satisfação a oportunidade de responder à primeira consulta pública organizada pela Autoridade Nacional de Proteção de Dados (ANPD) e gostaria de elogiar a ANPD por buscar cooperação e contribuições de múltiplas partes interessadas.

O CIPL é um think tank global que atua na área de privacidade e proteção de dados e segurança da informação com sede em Washington DC, Londres e Bruxelas, fundado em 2001 no escritório de advocacia Hunton Andrews Kurth LLP. A missão do CIPL é se engajar em liderança de ideias e promover boas práticas que garantam tanto a proteção efetiva da privacidade quanto o uso responsável dos dados pessoais na era moderna da informação. O trabalho do CIPL facilita o engajamento construtivo entre líderes empresariais, profissionais de privacidade e segurança, reguladores e tomadores de decisão em todo o mundo. Trabalhamos com líderes seniores e especialistas em privacidade de mais de 80 organizações globais líderes que nos fornecem casos concretos sobre suas práticas de privacidade de dados e tomada de decisões. Veja mais sobre o CIPL em https://www.informationpolicycentre.com/.

Nada nesta apresentação deve ser interpretado como representando a opinião individual de qualquer empresa membro do CIPL ou do escritório de advocacia Hunton Andrews Kurth.

CONTRIBUIÇÕES RECEBIDAS **IMPORTANTE:** Os comentários e sugestões referentes à tomada de subsídio deverão ser fundamentados e justificados. Caso seja citada experiência internacional, favor inserir o endereço eletrônico para acessar o instrumento normativo.	
TÓPICO/QUESTÃO	**CONTRIBUIÇÃO/INSTITUIÇÃO**
Quando um incidente pode acarretar risco ou dano relevante ao titular? Que critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante?	As atividades de tratamento de dados sempre apresentarão algum grau de risco para os indivíduos, que podem resultar de incidentes de segurança. As avaliações de risco incluem a análise da probabilidade e gravidade dos riscos aos direitos e liberdades dos indivíduos, incluindo quaisquer danos potenciais a indivíduos. Os riscos e danos associados a um incidente de segurança específico nem sempre estão correlacionados com o tamanho ou escopo do próprio incidente (por exemplo, o vazamento de dados financeiros de um pequeno número de pessoas pode ser mais danoso do que o vazamento de um número maior de dados que sejam comparativamente menos sensíveis). Os danos podem ser classificados em: • Danos materiais e imateriais – também conhecidos como danos tangíveis e intangíveis. A materialidade deve ser expressa em termos mensuráveis e objetivos, como valor monetário associado ao dano causado. Os danos materiais podem exigir priorização sobre os danos imateriais, dependendo do contexto; e • Danos sociais – a consideração de danos sociais (por exemplo, o público se abster de usar um aplicativo de rastreamento do COVID-19 no caso de haver um incidente de segurança amplamente divulgado na mídia relacionado a esse aplicativo) não é um requisito da LGPD e a ANPD não deve esperar que as organizações considerem os danos sociais em todas as suas avaliações de risco. No entanto, as organizações podem optar por considerá-los em circunstâncias específicas (no exemplo mencionado anteriormente, ao processar dados pessoais para combater a pandemia de COVID-19). A avaliação dos riscos e da probabilidade de danos no contexto de incidentes de segurança, a notificação de incidentes e a remediação devem ser consideradas como parte, ou um exemplo, das avaliações de risco mais amplas derivadas

	dos requisitos da LGPD. As organizações brasileiras estão obrigadas, nos termos do artigo 6, VII e VIII, a adotar medidas técnicas e administrativas para garantir a segurança de dados pessoais e evitar danos – essas seriam medidas de mitigação consideradas integrantes de uma avaliação de risco. O artigo 46 da LGPD vai além, obrigando controladores e operadores a adotarem medidas específicas de prevenção e gestão de incidentes. Essas medidas incluem avaliações de risco, bem como mitigação e controles implementados com base em avaliações de risco. As organizações não podem ser obrigadas a garantir a segurança absoluta das atividades de tratamento de dados; elas devem, porém, implementar medidas de segurança apropriadas ao risco de quaisquer danos potenciais previstos, conforme determinado pelas avaliações de risco. O gerenciamento de segurança é uma tarefa complexa que envolve uma ampla gama de fatores, dependendo do contexto e exigindo monitoramento contínuo de ameaças internas e externas. As ameaças externas, em particular, tornam-se mais sofisticadas a cada dia e podem ser imprevisíveis até mesmo para organizações mais maduras. Além disso, o risco de erro humano jamais pode ser totalmente excluído; só pode ser reduzido por meio de treinamento. **Portanto, a regulamentação da ANPD sobre incidentes de segurança deve ser flexível para dar conta dos contextos e variedades específicas de quaisquer incidentes de segurança e <u>não</u> deve ser prescritiva ou esperar que as organizações adotem metodologias específica, especialmente porque os riscos podem variar com o tempo e as metodologias podem ter que evoluir com as mudanças do cenário de risco. A ANPD pode, em vez disso, fornecer às organizações exemplos** de (i) quais poderiam ser os possíveis riscos e danos resultantes de diversos tipos de incidente de segurança, (ii) critérios não exaustivos que os controladores podem usar ao avaliar o nível de risco envolvido no incidente de segurança, e (iii) metodologias comumente adotadas no mercado para gerenciar incidentes de segurança (ver resposta à pergunta abaixo em “Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?”. Com isto, a ANPD poderá criar e facilitar o máximo de consistência possível, tendo em mente o contexto e a sensibilidade das avaliações de risco individuais e a consequente necessidade de flexibilidade. Em relação ao ponto (ii) no parágrafo acima e na segunda parte desta pergunta da ANPD, segue abaixo uma lista não exaustiva de critérios que as organizações geralmente levam em consideração ao avaliar o nível de risco de um incidente de segurança: • Probabilidade de ocorrência/materialização de danos a indivíduos como resultado do incidente – isto é importante para diferenciar entre incidentes em que os riscos para os titulares podem estar presentes mas a probabilidade de tais riscos ou danos realmente se materializarem é baixa, e incidentes em que os riscos estão presentes e a probabilidade de tais riscos ou danos se materializarem é significativa; • A gravidade dos possíveis danos a indivíduos (por exemplo, possíveis danos resultantes de incidentes em que os dados são revelados por acidente a uma parte confiável são provavelmente menos graves que os possíveis danos resultantes de incidentes em que os dados são revelados ao público em geral); • O tipo de incidente de segurança (por exemplo, quebra de sigilo por uma pessoa com acesso a dados, invasão de um sistema e, portanto, violação de sua integridade, indisponibilização de dados a seus usuários legítimos);

	• A natureza e sensibilidade dos dados pessoais (ou seja, quanto mais sensíveis os dados, maior será o risco de dano às pessoas afetadas, mas também devem ser considerados os dados pessoais que talvez já tenham sido tornados públicos pelo titular); • A facilidade com que os indivíduos podem ser identificados (por exemplo, se os dados pessoais foram criptografados e a chave de criptografia não foi divulgada, os riscos provavelmente serão muito menores); • Quaisquer características especiais do indivíduo afetado (por exemplo, dados referentes a crianças/outros indivíduos vulneráveis podem resultar em um risco maior do que dados de adultos); • Se o mesmo tipo de incidente já aconteceu no passado; e • As medidas tomadas pelo controlador para mitigar o impacto do evento. O CIPL acredita que vincular a determinação de notificar um incidente de segurança ao número de indivíduos potencialmente afetados pode ter consequências indesejadas. Por exemplo, um incidente com baixa probabilidade de causar danos a indivíduos pode ser interpretado como tendo uma classificação de risco mais alta caso o número de indivíduos potencialmente afetados seja alto, podendo resultar em notificação regulatória inadequada. O número de indivíduos afetados não é um bom indicador do dano real ou da probabilidade de dano que um indivíduo pode sofrer como resultado de um incidente de segurança. **A ANPD deve, portanto, exigir que as organizações realizem uma avaliação de risco do incidente de segurança, levando em consideração os critérios listados acima e quaisquer outros critérios relevantes para definir se devem notificar o incidente à ANPD e aos titulares dos dados. O artigo 48 da LGPD determina que as organizações devem notificar incidentes que possam resultar em riscos ou danos "relevantes". Ao interpretar este requisito, a ANPD deve considerar como "relevantes" apenas os riscos e danos que sejam (i) materiais e/ou (ii) classificados como de alto risco na avaliação de risco dos controladores** (ver resposta à pergunta abaixo). É necessário que a ANPD interprete a LGPD de maneira a garantir que o limite dos riscos e danos "relevantes" seja definido no nível correto, para que as organizações tenham que notificar apenas aqueles incidentes em que haja probabilidade de danos materiais a indivíduos e que sejam classificados como de alto risco. O CIPL incluiu abaixo alguns exemplos práticos de incidentes que não são materiais nem de alto risco e que, portanto, não devem ser considerados como notificáveis: • Um funcionário tem acesso acidental a um documento relacionado a um processo de recrutamento. Embora o documento possa conter dados pessoais que, se expostos mais amplamente, poderiam criar o risco de consequências adversas para o titular (por exemplo, em termos de vínculo com o empregador atual), a probabilidade de tal risco se materializar é baixa porque o funcionário está sujeito a requisitos de confidencialidade e notificou internamente o acesso acidental com o compromisso de excluir o documento.

<table>
<tr>
<td></td>
<td>

Alguns dados pessoais (como fotografias, informações sobre promoções profissionais, etc.) foram disponibilizados involuntariamente por meio do acesso a um link de URL temporário, mas compartilhável, em ferramenta de comunicação interna. Embora não se possa excluir por completo a possibilidade de que tal link seja usado por pessoa não autorizada a acessar tal conteúdo, a probabilidade deste risco ocorrer é minimizada pela validade temporária do link, bem como por medidas de moderação que limitam a natureza do conteúdo compartilhado na ferramenta. Além disso, os possíveis danos aos indivíduos não se materializaram.
Faturas incluindo detalhes de transações individualizadas (por exemplo, data, hora e local da compra) são compartilhadas equivocadamente num contexto business-to-business. Embora as informações contidas na fatura possam potencialmente levar à identificação de clientes, tal processo exigiria esforço de correspondência e acesso a conjuntos de dados externos. Além disso, o estabelecimento comercial está sujeito a obrigações de confidencialidade e compromete-se a não fazer nenhum uso posterior de tais informações.

</td>
</tr>
<tr>
<td>O risco ou dano relevante deveria ser subdividido em mais categorias (ex. Baixo, médio, alto etc.)? Como distinguir os níveis? Risco ou dano baixo deve ser considerado relevante ou não relevante?</td>
<td>
As organizações adotam diversas metodologias para realizar as avaliações de risco. Organizações maiores normalmente categorizam os níveis de risco ao realizarem tais avaliações, incluindo avaliações relacionadas a incidentes de segurança. Essas categorias geralmente são baixo risco/médio risco/alto risco, e algumas organizações também usam categorias extras, como sem risco/risco muito alto/risco muito baixo. São várias as metodologias usadas por organizações para medir o nível de risco associado a essas categorias. Organizações maiores também podem fazer uso de ferramentas que lhes permitam atribuir uma pontuação a cada uma dessas categorias e calcular objetivamente a pontuação final do evento usando critérios especificados (como os critérios descritos em nossa resposta à pergunta acima). Algumas organizações também utilizam uma matriz de risco, como a ilustrada abaixo. Conforme mencionado em nossa resposta à pergunta acima, o CIPL recomenda que apenas os riscos classificados como de alto risco sejam considerados notificáveis.

Abaixo segue um exemplo de matriz de probabilidade e gravidade que algumas organizações usam para avaliar os riscos envolvidos em incidentes de segurança:
<table>
<tr><th>PROBABILIDADE DE OCORRÊNCIA DE DANO
GRAVIDADE DO DANO</th><th>ALTA PROBABILIDADE</th><th>MÉDIA PROBABILIDADE</th><th>BAIXA PROBABILIDADE</th></tr>
<tr><td>ALTA GRAVIDADE</td><td>Alta probabilidade
Alta gravidade</td><td>Média probabilidade
Alta gravidade</td><td>Baixa probabilidade
Alta gravidade</td></tr>
<tr><td>MÉDIA GRAVIDADE</td><td>Alta probabilidade
Média gravidade</td><td>Média probabilidade
Média gravidade</td><td>Baixa probabilidade
Média gravidade</td></tr>
</table>
</td>
</tr>
</table>

	<table><tr><td rowspan="2">BAIXA GRAVIDADE</td><td>Alta probabilidade</td><td>Média probabilidade</td><td>Baixa probabilidade</td></tr><tr><td>Baixa gravidade</td><td>Baixa gravidade</td><td>Baixa gravidade</td></tr></table> **A ANPD <u>não</u> deve exigir que as organizações usem metodologias ou ferramentas específicas para avaliar os riscos relacionados a incidentes de segurança. A ANPD deve deixar que as organizações decidam quais metodologias e ferramentas de avaliação de risco são mais adequadas a seus respectivos contextos, desde que as organizações possam demonstrar que avaliaram os riscos de forma adequada** (por exemplo, organizações menores podem optar por avaliar os riscos informalmente com base em perguntas e experiência interna, enquanto organizações maiores podem implementar ferramentas mais complexas e até mesmo vincular essas avaliações à função geral de gerenciamento de risco corporativo). Os controladores devem ter a capacidade (mas não a obrigação) de construir matrizes de risco que funcionem para a sua organização. Pode ser útil, especialmente para organizações menores, que a ANPD forneça uma lista de verificação (checklist) ou uma lista de perguntas que indiquem se um incidente seria notificável (por exemplo, o incidente resultou em danos concretos e materiais a indivíduos? Envolveu dados pessoais sensíveis ou dados pessoais referentes a indivíduos vulneráveis?). A ANPD também poderia elaborar uma ferramenta que as organizações possam usar para avaliar os riscos (por exemplo, uma planilha com um sistema de pontuação), deixando claro que tal ferramenta é opcional e que as organizações podem desenvolver suas próprias ferramentas/metodologias ou usar ferramentas/metodologias terceirizadas. A ANPD também pode fornecer exemplos de quais são os riscos e danos que as organizações podem considerar, bem como estudos de caso envolvendo incidentes notificáveis e não notificáveis.
Como distinguir o risco ao titular do dano ao titular? Como esses conceitos se relacionam?	Riscos são a probabilidade ou possibilidade de ocorrência de danos. Quando houver risco de dano, existirá a possibilidade um dano real se materializar. Conforme explicado na pergunta acima, os danos podem ser materiais ou imateriais/tangíveis ou intangíveis. Um incidente de segurança pode revelar a existência de (i) um risco significativo, caso em que o evento danoso permanece latente, ou (ii) danos a indivíduos, caso em que há evidências suficientes de que o evento já produziu seus resultados danosos. Embora os conceitos de "risco" e "dano" sejam independentes, eles estão intrinsecamente relacionados para fins de avaliações de risco.
O que deve ser considerado na avaliação dos riscos do incidente?	Ver resposta à primeira pergunta acima em "Quando um incidente pode acarretar risco ou dano relevante ao titular? Que critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante?"
Quais informações os controladores devem notificar à ANPD, além daquelas já listadas no §1º do art. 48?	O artigo 48, parágrafo 1º, da LGPD estabelece uma lista suficientemente abrangente de informações que os controladores devem fornecer à ANPD e aos titulares ao notificarem incidentes de segurança. Não está previsto que a ANPD deva exigir o fornecimento de informações além do que consta nesta lista. **O CIPL recomenda que a ANPD <u>não</u> exija o fornecimento de informações adicionais específicas, mas que permita que os controladores decidam no caso a caso se o fornecimento de informações adicionais seria útil,** principalmente ao notificar o incidente à ANPD e cooperar com uma possível investigação da ANPD. Essas informações adicionais podem estar relacionadas, por exemplo, às complexidades de um incidente de alcance global envolvendo várias jurisdições e/ou outros terceiros.

Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)	O artigo 48, parágrafo 1º, da LGPD determina que os controladores devem comunicar, "em prazo razoável", à ANPD e aos titulares a ocorrência de incidentes de segurança que possam acarretar riscos ou danos relevantes para os titulares, e que a ANPD pode definir esse prazo. O regulamento da ANPD deve estabelecer limites claros de notificação, especialmente para incidentes menores, e evitar definir um limite baixo para a notificação. A notificação de incidentes é uma atividade que pode consumir muitos recursos, dependendo do porte e da complexidade da organização. Isso pode resultar em significativo ônus financeiro e administrativo para as organizações, agravado pelo aumento de ameaças e ataques externos. Se o limite para notificação for muito baixo, os recursos que poderiam ser gastos para ampliar os processos de conformidade internos e proteger os indivíduos podem ser mal direcionados. A ANPD pode ficar tentada a seguir o padrão de 72 horas/três dias estabelecido pelo artigo 33 do Regulamento Geral de Proteção de Dados da UE (RGPD). É importante, no entanto, que a ANPD reconheça que nem todas as disposições do RGPD são realistas. A ANPD não precisa seguir os exemplos da UE em todas as instâncias, e sim seguir apenas aqueles exemplos que são eficazes e fornecem o mais alto nível de proteção aos indivíduos, considerando também as particularidades do contexto brasileiro – ver relatório da Hunton Andrews Kurth: Seeking Solutions: Aligning Data Breach Notification Rules Across Borders (Em busca de soluções: alinhando as regras de notificação de violação de dados entre fronteiras), que destaca as principais diferenças e oportunidades de convergência nos regimes de notificação de violação de dados existentes ao redor do mundo. 72 horas ou três dias (ou mesmo dois dias, conforme recomendação provisória da ANPD em seu site) não é tempo suficiente para uma organização compreender totalmente o escopo e a extensão de um incidente de segurança e, portanto, definir se deve ou não ser notificado. Por causa disso, as organizações da UE muitas vezes notificam preventivamente a autoridade de proteção de dados da ocorrência de violação de dados, apenas para parar o cronômetro, o que resulta em supernotificação e custos associados de tempo e recursos (ver a contribuição do CIPL no Multistakeholder Expert Group to the Commission 2020 Evaluation of the GDPR (Grupo de Especialistas Multissetoriais para a Avaliação da Comissão 2020 do RGPD), página 36. Na verdade, prazos fixos para notificação de incidentes de segurança podem ter uma série de consequências indesejadas: • Precipitar notificações por medo de sanções, antes que uma avaliação completa dos eventos possa ser realizada, resultando em supernotificação de incidentes à ANPD, incluindo a notificação de incidentes que são incidentais e que no fim acarretam apenas baixo ou médio risco. A notificação apressada e prematura também não promove boas práticas de responsabilidade de prestação de contas (accountability) para as organizações que notificarão mecanicamente a ANPD para se protegerem em vez de realizar avaliações de boa-fé levando em consideração a probabilidade e gravidade do risco para os indivíduos; • Criar um falso senso de urgência que possa inadvertidamente resultar em uma situação em que a notificação deve ser complementada ou retificada conforme a avaliação evolui;

	• Transferir recursos da contenção e mitigação do incidente para a notificação deste (o que é particularmente relevante em organizações de pequeno e médio porte com recursos limitados); e • Criar o risco de responsabilização legal (liability) para a organização, mesmo quando ela estiver agindo com o maior padrão de diligência e cuidado. Permitir que as organizações tenham mais tempo para realmente entender o que aconteceu, avaliar o verdadeiro risco do incidente e lidar com ele de forma adequada fará com que a ANPD receba relatórios de melhor qualidade e provavelmente menos notificações, pois os controladores saberão dizer com mais certeza se a notificação do incidente é cabida ou não. Frequentemente, há um atraso prático entre o momento em que o funcionário toma conhecimento de uma violação e o momento em que o funcionário responsável pelas questões de proteção de dados é devidamente informado. Além disso, uma avaliação confiável de risco incluirá uma análise forense detalhada para determinar a probabilidade e a gravidade dos danos aos indivíduos e avaliar a necessidade de notificação. Nos cenários mais complexos, e em particular aqueles que envolvem ataques externos sofisticados, as investigações podem ocorrer durante várias semanas antes que os fatos (mesmo os fatos básicos, como a existência de qualquer possibilidade de acesso não autorizado aos dados) possam ser determinados. Veja, por exemplo, o 2020 BakerHostetler Data Security Incident Response Report (Relatório de Resposta a Incidentes de Segurança de Dados de 2020 da BakerHostetler), que mostra que o tempo desde a descoberta do incidente até a notificação leva em média 38 dias. O 2020 Verizon Data Breach Investigations Report (Relatório de investigações de violação de dados de 2020 da Verizon) indica que as violações de dados levam meses ou mais para serem descobertas em grandes organizações, enquanto, em organizações de pequeno porte, esse tempo é menor. O CIPL, portanto, apoia o padrão da LGPD de não estabelecer prazo fixo para a notificação de incidentes de segurança e, em vez disso, colocar sobre o controlador o ônus de garantir que a notificação seja emitida em tempo hábil e adequado à natureza e ao nível de risco envolvido no incidente. **O CIPL recomenda que a ANPD (i) mantenha o padrão existente da LGPD de prazo aberto, mas "razoável", e que (ii) forneça orientações e exemplos adicionais (ou seja, casos de uso) para ilustrar quando uma organização "toma conhecimento" de um incidente, o que seria considerado como notificações em tempo hábil e como as organizações podem demonstrar o cumprimento do cronograma e a adoção das devidas medidas para conter e remediar o incidente com eficácia.** Caso a ANPD decida não incorporar esta sugestão, o CIPL sugere que o prazo mínimo para notificação seja de 3 dias úteis a partir do momento em que a organização tome conhecimento do incidente, levando em consideração os dias úteis de funcionamento da empresa. A ANPD também deve fornecer orientações sobre o que significa "tomar conhecimento" do incidente e, portanto, em que ponto começa a contagem do tempo para a notificação à ANPD. Em vez de exigir notificação dentro de um prazo razoável a partir do conhecimento do incidente, o CIPL recomenda iniciar o cronômetro a partir do momento em que o incidente foi (ou razoavelmente deveria ter sido) confirmado, com orientação clara sobre qual nível de certeza razoável os controladores devem ter em relação à real ocorrência do incidente.

	Além disso, a ANPD deve considerar que as mesmas pessoas responsáveis por mitigar os incidentes de segurança são também responsáveis por fornecer as informações necessárias para a notificação. Assim, a ANPD não deve priorizar a notificação sobre a remediação, pois isso poderia ser pior para os titulares. Isto é ainda mais relevante para entidades menores com menos recursos.
Qual seria um prazo razoável para que os controladores informem os titulares de dados sobre o incidente de segurança? (art. 48, §1º) Que informações devem constar dessa comunicação? As mesmas do §1º do art. 48?	Ver a pergunta anterior para considerações sobre o prazo razoável de notificação. As mesmas considerações se aplicam à comunicação a indivíduos. Em particular, o CIPL recomenda que a ANPD exija que os controladores notifiquem os titulares "dentro de um prazo razoável" apenas quando houver confirmação de que os titulares estejam sujeitos a riscos de danos materiais à privacidade classificados como de alto risco, e o controlador está em posição de aconselhar sobre as medidas de proteção que os titulares podem tomar (ou seja, para reduzir o risco de danos ou os danos em si, case já tiverem materializados). Isso evitaria a "fadiga da notificação", que poderia resultar de constantes notificações sobre incidentes irrelevantes. Notificações constantes ou frequentes iriam, de fato, prejudicar a proteção dos indivíduos, pois prejudicaria a capacidade, ou até mesmo disposição, deles de diferenciar continuamente entre situações que requerem ação de sua parte para se protegerem e situações em que o risco de dano é trivial e nenhuma ação é necessária. A comunicação em fases também pode ser razoável, desde que não sobrecarregue ou cause ansiedade desnecessária aos titulares. Nos casos em que os titulares precisam ser informados para que eles próprios possam tomar medidas de mitigação, faz sentido notificá-los o quanto antes, desde que isso seja viável. Em relação ao conteúdo da comunicação, as informações enumeradas no artigo 48, parágrafo 1º, da LGPD são suficientes. O conteúdo e o estilo desta notificação não devem, no entanto, ser iguais ao conteúdo da notificação à ANPD, visto que elas têm finalidades diferentes. Quaisquer requisitos obrigatórios em termos do conteúdo da notificação devem ser interpretados de forma flexível e não entendidos como requisito para citar a LGPD. A ANPD deve, portanto, fornecer as seguintes orientações aos controladores: • A comunicação deve ser escrita em linguagem clara e simples, evitando termos técnicos e jurídicos, deve ser concisa e amigável (por exemplo, a ANPD pode recomendar uma abordagem em camadas para que os titulares obtenham mais informações, se desejarem); • A comunicação deve ser independente de outras comunicações emitidas pelo controlador (por exemplo, um e-mail específico em vez de parte de um e-mail com ofertas de produtos e serviços); • A comunicação deve evitar linguagem alarmante e concentrar-se nas medidas que os titulares podem tomar para se protegerem ainda mais; e • As informações fornecidas sobre as medidas de mitigação que foram ou serão adotadas devem ser limitadas a um nível que seja útil para os indivíduos (observe que fornecer muitos detalhes pode abrir portas para que atores mal-intencionados contornem os planos de remediação). Seja qual for o caso, o requisito de comunicação não deve ser utilizado como meio para penalizar o controlador que sofreu o incidente de segurança (por exemplo, prejudicar sua reputação pública). O foco da comunicação deve ser o

	indivíduo afetado e o conteúdo deve se limitar a informações úteis que o ajudem a se proteger, conforme previsto no artigo 48, parágrafo 1º.

Qual a forma mais adequada para a realização da comunicação do incidente aos titulares? A comunicação deve ser sempre direta e individual (por via postal, e-mail etc.) ou, em determinadas circunstâncias, pode ser admitida a comunicação pública (nota à imprensa, publicação na internet etc.)?	Não há um padrão ou uma abordagem única que sirva para todos para notificação de incidentes de segurança com titulares de dados. Os controladores são os mais bem posicionados para saber como se comunicar de forma mais eficaz com seus usuários/titulares de dados e podem ter suas próprias maneiras de efetivar tais comunicações. A eficácia da comunicação deve ser o critério principal para notificação, mais que um formato pré-determinado. Preferencialmente, a notificação deve seguir o método com o qual o controlador regularmente interage com o titular dos dados.
	
	O CIPL recomenda que a ANPD (i) não exija um tipo específico de notificação, mas em vez disso forneça exemplos aos controladores sobre como eles podem notificar titulares de dados, e (ii) reconheça que os esforços envolvidos na notificação devem ser apropriados para o nível de risco e as circunstâncias específicas do caso. A ANPD deve informar os controladores que eles devem escolher o tipo de notificação mais apropriado para atingir a meta de informar indivíduos sobre o incidente e permitir que eles tomem quaisquer medidas necessárias (p. ex., mudar suas senhas) para manter seus dados pessoais protegidos. Alguns exemplos incluem:
	
	• Quando titulares de dados são identificados/individualizados e o controlador tem relação direta com eles:
	  ○ Carta enviada por correio;
	  ○ E-mail;
	  ○ SMS;
	  ○ Notificação por aplicativo ou plataforma (p. ex., pop-ups ou banners).
	
	• Excepcionalmente, a ANPD deve permitir notificações públicas quando (i) os titulares de dados não são identificados/individualizados, (ii) o controlador não tem uma relação direta com eles, (iii) os meios habituais de comunicação se tornaram inacessíveis em razão de um incidente (p. ex., o titular dos dados perdeu acesso ao e-mail), (iv) identificar e notificar os indivíduos demandaria um esforço desproporcional (p. ex., envolvendo custos proibitivos) e (v) a notificação deve ser urgente devido ao caráter de alto risco do incidente específico. Os exemplos incluem:
	  ○ Postagem em website; e
	  ○ Comunicações através de canais de mídia (tais como sites relevantes de notícias e TVs).
	
	• Adicionalmente, a ANPD deve considerar que pode haver instâncias em que os titulares de dados são identificados, mas não é possível notificar todos eles (p. ex. quando contas de e-mail foram fechadas ou o indivíduo trocou de endereço e não atualizou o novo endereço no sistema do controlador). Uma notificação pública pode não ser adequada nestes casos, pois apenas serviria para causar mais ansiedade ao invés de

	oferecer informações aos indivíduos impactados. Nestes casos, a ANPD não deve exigir que o controlador comunique o incidente publicamente.
Quais seriam as eventuais exceções da obrigatoriedade de informar a ANPD?	Não se deve exigir que os controladores notifiquem a ANPD sobre incidentes de segurança que/onde: • For improvável que resultem em alto risco de prejuízo real aos indivíduos de acordo com a metodologia de risco aplicada pelo controlador (veja a resposta à primeira questão); • Envolverem apenas dados não pessoais (incluindo dados anônimos), na medida em que a LGPD cobre apenas a proteção de dados pessoais; • Envolverem dados pessoais que tenham se tornado ininteligíveis ou inidentificáveis antes do incidente e não há risco que dados sejam reidentificados (p. ex., criptografia onde a chave não tenha sido revelada, dados anônimos); • Envolverem a revelação involuntária de dados pessoais apenas para uma terceira parte confiável; e • Imediatamente após o incidente o controlador tenha tomado ações/medidas mitigatórias que asseguram que o nível de risco exigido para desencadear uma notificação aos titulares de dados não esteja mais presente.
Quais seriam as possíveis exceções da obrigatoriedade de informar os titulares?	Adicionalmente às isenções listadas acima, não se deve exigir que os controladores notifiquem os titulares de dados sobre incidentes de segurança que/onde: • Tenham sido eficazmente mitigados pelo controlador depois que se tornou ciente do evento e, consequentemente, não mais apresente riscos de prejuízos aos titulares de dados; • A materialização de riscos e prejuízos a indivíduos for improvável; • Envolvam apenas dados pessoais que já estejam em domínio público; • Emitir tais notificações impediria uma investigação criminal; e • Um dos controladores associados em uma relação de processamento de dados não tem as informações identificadoras dos titulares de dados (p. ex. operadores de redes de cartão de crédito que são controladores associados com emissores de cartões de crédito e teriam apenas os números de cartões sem os dados de identificação). Nestes casos, a ANPD não deve requerer que este controlador associado notifique titulares de dados. Isto deve ser responsabilidade do outro controlador associado que detém a informação identificadora dos titulares de dados.
Quais são os possíveis critérios a serem adotados pela ANPD na análise da gravidade do incidente de segurança? (art. 48, §2º)	Veja a resposta na primeira questão acima, em "Quando um incidente pode resultar em riscos ou danos relevantes para titulares de dados? Que critérios a ANPD deveria levar em conta para considerar relevantes os riscos ou danos?"

Existe alguma metodologia recomendada para a análise de gravidade do incidente de segurança? Se sim, qual(is)?	As três metodologias mais usadas para se avaliar incidentes de segurança e gerenciar riscos relacionados a processamentos de dados são: • Agência Europeia para a Segurança das Redes e da Informação (ENISA), Recommendations for a methodology of the assessment of severity of personal data breaches (Recomendações para uma metodologia de avaliação da gravidade das violações de dados pessoais), 20 de dezembro de 2013; • Organização Internacional para Padronização (ISO), ISO 31000 – risk management (ISO 31000 – gestão de risco); e • Instituto Nacional de Padrões e Tecnologia (NIST), NIST Privacy Framework: a Tool for Improving Privacy Through Enterprise Risk Management (Estrutura de Privacidade do NIST: uma ferramenta para melhorar a privacidade através da gestão de risco corporativo), versão 1.0, 16 de janeiro de 2020. Organizações brasileiras deveriam, entretanto, ter a capacidade de construir um processo de gerenciamento de incidentes adequado à sua estrutura, natureza de negócios e quadros de trabalho de gerenciamento geral de riscos. As metodologias para avaliar a severidade de incidentes de segurança podem ser usadas como materiais especializados de referência, mas não devem ser tratadas como um componente compulsório de um processo de gerenciamento de incidentes que seja visto como conforme com a LGPD.
Quais seriam sugestões de providências, incluindo medidas técnicas e administrativas, a serem determinadas pela ANPD aos controladores após a comunicação do incidente de segurança?	O Artigo 48, parágrafo 2, II da LGPD estipula que a ANPD pode requerer dos controladores a adoção de medidas que revertam ou mitiguem os efeitos de um incidente de segurança. O CIPL recomenda, contudo, que, em vez de requer dos controladores que tomem medidas específicas, a ANPD faça recomendações de tais medidas ou exija que os controladores definam estas medidas e as apresente à ANPD (p. ex. em um documento). Isto acontece porque os controladores estarão mais bem equipados para saber quais seriam as medidas mais eficazes e teriam um entendimento melhor dos aspectos técnicos envolvendo o incidente de segurança. De modo semelhante, no caso de a ANPD recomendar (ou definitivamente requerer) que medidas específicas sejam tomadas, os controladores devem ser capazes de ponderar sobre tais medidas e propor outras mais adequadas. **Os controladores devem, assim, desempenhar um papel prioritário na determinação de medidas mitigatórias e o papel da ANPD deve ser o de oferecer uma validação geral sobre a suficiência de tais medidas remediadoras, levando em consideração requerimentos de segurança razoáveis.** Isto é particularmente relevante para controladores que sejam grandes organizações. Medidas que a ANPD pode recomendar incluem: • Tomar decisões rápidas para conter o incidente, tais como desativar o sistema, isolando-o da rede, e desativar certas funções; • Medidas destinadas a resolver certos efeitos do incidente de segurança, tais como eliminar malware ou desativar contas comprometidas; • Minimização de Dados;

	• Medidas para restaurar completamente serviços a seus níveis normais e evitar, tanto quanto possível, que ocorram quaisquer novos incidentes relacionados à mesma causa; • Medidas para evitar que incidentes semelhantes aconteçam no futuro, tais como melhorar a segurança de sistemas e criar políticas e procedimentos internos, aumento de privacidade e treinamento em segurança da informação, auditorias, tratamento de vulnerabilidades internas, implementação de um programa de governança de dados abrangente e de responsabilidade por prestação de contas (accountability). • Reunião e custódia de provas para conter e reverter o impacto do incidente; e • Documentação do incidente e de medidas tomadas.
Considerações adicionais relacionadas ao gerenciamento e à notificação de incidentes de segurança	• **A ANPD deve levar em conta a accountability como um fator mitigatório ao executar a LGPD em seguida a uma notificação de incidente de segurança** — particularmente nos casos em que o controlador tenha tomado atitudes abrangentes e eficazes para conter e mitigar os riscos e tenha sido capaz de demonstrar estas enquanto colabora com a ANPD. Ter uma arquitetura de accountability dentro de uma organização é essencial para se avaliar riscos relevantes, implementar um nível de segurança apropriado aos riscos, elaborar políticas e procedimentos de gerenciamento de crise, treinamento de empregados, desempenhar a devida diligência (due dilligence) do operador, auditar práticas e responder a um incidente de segurança. Veja, por exemplo, o Accountability Framework do CIPL no documento oficial "The Case for Accountability: How it Enables Effective Data Protection and Trust in the Digital Society" ("O caso a favor da responsabilidade por prestação de contas/accountability: como ela permite a efetiva proteção de dados e a confiança na sociedade digital"). • **Um incidente de segurança não é um indicador de proteção insuficiente de dados pessoais** — é importante que a ANPD entenda que o fato de apenas ter havido um vazamento não significa necessariamente que as medidas de segurança organizatórias e técnicas adotadas foram insuficientes. Cada incidente e as medidas de segurança implementadas precisam ser considerados em suas próprias circunstâncias. A ANPD deveria reconhecer que perfeição não é o padrão em segurança de informação. Padrões de segurança industrial são pensados como marcos que assegurem que as entidades estão gerenciando riscos adequadamente. Eles não devem ser entendidos normativamente, porque isso pode de fato diminuir a segurança ao consumir recursos e perder o foco em riscos críticos. • **Operadores não devem ser os que determinam se deve haver uma notificação de violação de dados** — quando a ANPD publicou a consulta pública em discussão, também publicou (i) um guia preliminar sobre violações de dados em que estabelecia que "[a]pesar de a responsabilidade e obrigação de relatar à ANPD ser do controlador, se a informação é excepcionalmente apresentada pelo operador, essa será devidamente examinada pela ANPD"; e (ii) um modelo da notificação com um campo a ser marcado pela entidade notificadora para informar se trata-se de controlador ou operador. O artigo 48, parágrafo 1 da LGPD é claro em dispor que o controlador deve notificar a ANPD sobre violações de dados. Controladores, com apoio de seus

	operadores na medida do necessário, estarão mais bem equipados para avaliar extensivamente a severidade da violação de dados e examinar os impactos potenciais que isso possa causar aos titulares de dados. Os controladores devem ser aqueles que determinam se a violação deve ser notificada à ANPD e aos titulares de dados. A respeito disso, o CIPL recomenda fortemente que a ANPD não sugira ou deixe implícito que os operadores deveriam ter de notificar a autoridade ou os titulares de dados. A ANPD poderia, em vez disso, recomendar que operadores notifiquem controladores sobre incidentes de segurança envolvendo seus dados pessoais e cooperar para fornecer aos controladores a informação relevante, assim como gerenciar o incidente. A ANPD poderia ainda recomendar que isso seja incluído no contrato entre controlador e operador. • **A ANPD deveria apenas proativamente contactar organizações depois de elas terem razoável certeza de que, sob sua seu mecanismo de avaliação de risco, um incidente é notificável.** A ANPD pode receber reclamações e questões de indivíduos a respeito de incidentes de segurança sobre os quais eles ficaram a par através de meios que não sejam a notificação formal de acordo com a LGPD. Nem todos estes incidentes ultrapassarão o limiar de notificação que a ANPD vai estabelecer. A ANPD não deveria estar tentada a seguir todos estes casos, mas em vez disso apenas aqueles a respeito dos quais há razoável certeza de que atingem os limiares de notificação.
Diretrizes regulatórias e materiais de referência recomendados	Diretrizes regulatórias recomendadas: • Data Protection Commissioner (DPC), da Irlanda, Guidance Note: A Practical Guide to Personal Data Breach Notifications under the GDPR (Nota de orientação: um guia prático para notificações de violação de dados pessoais sob o RGPD), outubro de 2019; • UK Information Commissioner's Office (Gabinete do Comissário de Informação) do Reino Unido, guidance on personal data breaches; (orientação) e • O Comitê Europeu de Proteção de Dados está atualmente atualizando suas Guidelines 01/2021 on Examples regarding Data Breach Notification (Diretrizes 01/2021 sobre exemplos relacionados à notificação de violação de dados) e a ANPD deveria seguir seus desenvolvimentos. Artigos do CIPL: • CIPL Response to the EDPB's Guidelines on Examples Regarding Data Breach Notification (Resposta do CIPL às diretrizes do EDPB sobre exemplos relacionados à notificação de violação de dados), 2 de março de 2021 • CIPL Comments on WP29's Breach Notification Guidelines (Comentários do CIPL sobre as diretrizes do WP29 sobre notificação de violação), 1 de dezembro de 2017

	• Documento oficial: Risk, High Risk, Risk Assessments and Data Protection Impact Assessments under the GDPR (Risco, alto risco, avaliações de risco e avaliações sobre o impacto da proteção de dados sob a LGPD), 21 de dezembro de 2016.

SUGESTÕES DE DISPOSIÇÕES
O CIPL não tem sugestões.