RIO DE JANEIRO, 2021

Consulta Pública ANPD:
O Dever de Comunicação de Incidentes de Segurança

GREAT for PARTNERSHIP
BRITAIN & NORTHERN IRELAND

ITS
Instituto de Tecnologia & Sociedade do Rio

1. RESUMO EXECUTIVO

Números de telefones, nomes completos, localizações, data de nascimento, biografia, endereços de e-mails, CPFs, salário, estado civil, FGTS, título de eleitor, escolaridade e até foto de rosto e classe social. São todos dados pessoais expostos recentemente, seja no vazamento que envolveu 220 milhões de brasileiros, ou 100 milhões de dados de celulares ou no vazamento do Superior Tribunal de Justiça. Manchetes de "Como saber se seus dados foram vazados?" já se tornaram corriqueiras nos principais veículos de mídias e exemplos de megavazamentos não faltaram nos últimos tempos.

É importante notar que por trás de vazamentos existe também um negócio lucrativo que os alimenta. Dados são hoje possivelmente o *commodity* mais desejado: quanto maior o volume de dados se detêm, maior o poder na economia movida a dados. Em razão disso, os vazamentos de dados decorrentes de incidentes de segurança têm se tornado cada vez mais frequentes, principalmente no Brasil. O estudo recente do Massachusetts Institute of Technology ("MIT") aponta que vazamentos de dados aumentaram 493% no Brasil, sendo que mais de 205 milhões de dados brasileiros vazaram de forma criminosa em 2019. Em número de incidentes relevantes, o país saltou de 3, em 2018, para 16 em 2019, de acordo com a pesquisa.

Diante desse cenário, o desafio posto é como lidar com os incidentes de segurança no país. A Lei Geral de Proteção de Dados (Lei nº 13.709/2019 ou "LGPD") é um grande passo para conferir segurança jurídica aos incidentes cibernéticos por reconhecer a necessidade de medidas técnicas e administrativas para proteger os usuários. Na mesma linha, o papel da Autoridade Nacional de Proteção de Dados (ANPD) de educação, apoio, regulamentação, fiscalização e governança do volume significativo de incidentes é primordial para a solução do desafio posto.

Nesse sentido, a ANPD iniciou o processo de tomada de subsídios para a regulamentação do dever de comunicação de incidentes de segurança. O esforço voltou-se para delimitação de critérios no que tange: a gravidade, classificações de riscos ao titulares, detalhes sobre as comunicações dos incidentes tanto à autoridade como aos titulares.

A consulta contou com contribuições da sociedade civil sobre o tema tão proeminente que integra a agenda regulatória do biênio 2021/2022 da ANPD, divulgada em 28 de janeiro de 2021. A partir dos subsídios reunidos, a autoridade realizará consulta pública e futuramente é esperado que as orientações para incidentes de segurança sejam conhecidas até julho/2021.

O ITS participou da Tomada de Subsídios, endereçando desafios voltados para a adequação nesse setor - dificuldades orçamentárias, técnicas e de implementação -, apresentando as oportunidades e mapeando algumas experiências internacionais neste tema, tais como a da União Européia, Reino Unido e Canadá.

É partindo desse contexto que compartilhamos, a seguir, os comentários submetidos à Autoridade.

PRINCIPAIS RECOMENDAÇÕES

1. **Estruturar um processo interno para lidar com o volume expressivo de incidentes.** O processo ideal seria que a autoridade funcionasse na lógica de "governo como plataforma" e desenvolvesse uma verdadeiro mecanismo que permitisse a ANPD ser elemento central da segurança da informação e intermediar e supervisionar a interação entre os atores.

2. **Utilizar ferramentas de formulários para lidar com grandes volumes,** por exemplo "*typeforms*" ou meios de pesquisa ("*surveys*"), que auxiliam a estruturar o envio e intermediação de notificações de incidentes, assim não só os dados obtidos são sistematizados automaticamente, o que facilita a todas as partes, como também criam uma metodologia e um caminho claro para os fluxos de informações sobre incidentes.

3. **Estabelecer opções de resposta mais institucionalizadas.** Na busca de manter a interação contínua com os titulares e controladores no processo de comunicação dos incidentes, é importante instituir opções de "*feedbacks*" seja em uma plataforma própria, seja em outro mecanismo desenvolvido para tal.

4. **Cooperar com outras entidades para guiar as investigações de incidentes.** Não é necessário que a autoridade seja o braço de investigação em todos os sentidos e para todos os casos.

5. **Reportar de forma constante e permanente a situação de incidentes de segurança.** Por meio das ferramentas automatizadas sugeridas previamente, a autoridade deve oferecer respostas e informações sobre a situação atual de incidentes de segurança no país.

6. **Publicar as investigações realizadas.** No intuito de facilitar a exponencialização do impacto e mitigar a complexidade das obrigações, a autoridade deve publicar, na medida do possível, as investigações. Essa transparência tem um impacto positivo na legitimidade e tende a gerar confiança do papel da ANPD.

SUMÁRIO

1. QUAIS SERIAM SUGESTÕES DE PROVIDÊNCIAS, INCLUINDO MEDIDAS TÉCNICAS E ADMINISTRATIVAS, A SEREM DETERMINADAS PELA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS AOS CONTROLADORES APÓS A COMUNICAÇÃO DO INCIDENTE DE SEGURANÇA?

A Estruturação de um Processo interno

O histórico dos últimos meses com um número significativo de incidentes de segurança (no Superior Tribunal de Justiça, mais 223 milhões de CPFs, mais de 100 milhões de dados de celulares, entre outros) somados ao exemplo europeu, em que houve aumento considerável no número de notificações na União Europeia após a entrada em vigor do Regulamento Europeu de Proteção de Dados ("GDPR") indicam números elevados tanto de incidentes como de notificações à ANPD. Dessa forma, potencialmente um dos principais desafios para a autoridade recém formada será receber, responder e resolver notificações de incidentes de segurança que virão em grandes volumes e possivelmente em crescente complexidade.

Nesse sentido, as soluções passam em visualizar a atuação da ANPD de duas maneiras: 1) como plataforma (dentro de um conceito de "governo como plataforma") ou 2) como prestadora de um serviço essencial (dentro de um conceito de "governo como serviço"). Para tratar dos grandes volumes de notificações, a lógica de plataforma permite que a organização, ainda que diminuta, possa ter um papel central na lida com incidentes de segurança da informação. Pode se apoiar em outras entidades e servir de facilitadora do processo. Nos casos de maior complexidade, por outro lado, a autoridade pode ter que desenvolver as suas capacidades internas para desenvolver os serviços que lhe são requeridos.

(A) Como lidar com grandes volumes:

O conceito de governo como plataforma, cunhado pelo americano Chris O'Reilly, é a primeira saída para o desafio do volume de notificações. O governo serve de infraestrutura informacional a permitir a reutilização de informações para construir novas aplicações úteis para a sociedade.

Nesse sentido, a ANPD pode servir como ponto focal da comunicação de incidentes, mas não necessariamente concentrar todas as etapas do atendimento às comunicações de incidentes de segurança. De um modo geral, deve estruturar um processo simples, acessível e claro para que os diferentes atores do sistema possam se coordenar facilmente. Tenha-se claro que o objetivo nesses casos é diminuir tanto os riscos como os danos propriamente ditos derivados de incidentes de segurança. As formas de sanção servem mais que tudo por seu efeito educacional de evitar a reincidência.

O processo ideal seria que a autoridade desenvolvesse uma verdadeira plataforma que permitisse a ANPD meramente intermediar e supervisionar a interação entre os atores. A título exemplificativo, a plataforma Consumidor.gov.br, serviço que permite a interlocução direta entre consumidores e empresas para solução de conflitos de consumo pela internet, é um ponto de referência. O monitoramento é realizado pelos órgãos de defesa do consumidor e pela Senacon. São mais de 2 milhões de reclamações registradas e 580 empresas participantes. Atualmente, 80% das reclamações registradas na plataforma são solucionadas pelas empresas, que respondem às demandas dos consumidores em um prazo médio de 7 dias.

Da mesma forma que a relação entre empresas e consumidores é intermediada pela plataforma mencionada acima; a relação entre controladores e titulares poderia seguir o mesmo caminho. Assim, a ANPD estaria no centro da resolução de incidentes de segurança, auxiliando tanto aos controladores, como permitindo um espaço seguro de contato com os titulares de dados.

Cabe reconhecer que implementar o governo como plataforma, nos termos mencionados, pode exigir certo aporte técnico e ser mais adequado como solução a longo prazo. Nesse sentido, medidas mais rápidas também devem ser consideradas:

Utilizar ferramentas de formulários, como *typeforms* ou *surveys*, para estruturar o envio de notificação de incidentes, assim os dados obtidos são sistematizados automaticamente, o que facilita a todas as partes. Por um lado, os controladores têm claro o tipo de informação que necessitam enviar e, por outro, permite que a ANPD tenha uma visão padronizada das ocorrências; o que facilita na elaboração de relatórios e em avaliações de impacto.

A proposta atual de formulário é um passo na direção correta, no entanto, a utilização de ferramentas automatizadas diminui a burocracia além de aumentar a eficiência da ação da autoridade.

Estabelecer opções de resposta mais institucionalizadas. Na busca de manter a interação contínua com os titulares e controladores no processo de comunicação dos incidentes, é importante instituir opções de feedbacks na própria plataforma. Essas respostas e/ou informações podem servir tanto para notificação de incidentes de segurança como denúncias de titulares. Vale inspiração em experiências internacionais como a plataforma da autoridade do Reino Unido que oferece uma auto avaliação para incidentes de segurança, checklists sobre como se preparar ou responder um incidente e exemplos didáticos de mitigação de danos.

Cooperar com outras entidades para guiar as investigações de incidentes. Não é necessário que a autoridade seja o braço de investigação em todos os sentidos e para todos os casos. Neste caso, a aplicação de governo como plataforma significa encontrar meios de guiar investigações com o auxílio de parceiros. É notável salientar que a Lei Geral de Proteção de Dados (LGPD), em seu art. 55-J, §4º, incentiva a prática aqui sugerida, isto é, ações de cooperação com órgãos e entidades da administração pública, a fim de facilitar as diferentes competências da ANPD (regulatória, fiscalizatória e punitiva).

Cumpre enfatizar que a autoridade de certa forma já atuou de maneira colaborativa - ainda que *ad hoc* - quando abriu procedimento com a colaboração de órgãos como a Política Federal para investigar o vazamento de 223 milhões de CPFs.

Similarmente, o acordo de cooperação com a Senacon para proteção de dados de consumidores é um movimento no sentido de atuar como plataforma, em que colabora com outros órgãos e autoridades no sentido de satisfazer o seu mandato, qual seja, o de assegurar a proteção de dados pessoais.

A sugestão é que tal medida seja replicada com outras entidades para auxiliar na lida com incidentes de segurança. Vale uma nota que ao tratar de segurança da informação, poderia ter um impacto positivo se fosse levada em consideração a participação e a colaboração com os diferentes setores, incluindo, em situações cabíveis o setor privado, a sociedade civil ou mesmo a academia e o corpo técnico.

(B) Como lidar com a complexidade:

O uso da lógica de plataforma faz com que seja possível a autoridade concentrar-se nos pontos que efetivamente sejam de sua responsabilidade final e que tenha maior especialidade. Nesse sentido, pode lidar com diferentes níveis de complexidade e lançar investigações próprias, por exemplo, somente nos casos que sejam efetivamente necessárias.

Nesse contexto, há um elemento significativo que não deve ser ignorado. Há uma necessidade de transparência e de dar respostas. Isso começa com um espaço em que a autoridade deixa claro tanto o cenário atual como a sua atuação. O adágio clássico de “não basta ser fiel, mas deve aparentar também o ser” é um imperativo nessas situações.

Para tanto as seguintes iniciativas são relevantes:

Reportar de forma constante e permanente a situação de incidentes de segurança. Por meio das ferramentas automatizadas sugeridas previamente, a autoridade deve oferecer respostas e informações sobre a situação atual de incidentes de segurança no país. A partir desses dados, a comunidade científica, terceiro setor e outras entidades podem estudar estratégias, avaliações e colaborações com a autoridade. Com isso, avaliações e aprimoramentos serão favorecidos.

Publicar as investigações realizadas. Um elemento que facilita a exponencialização do impacto é a clareza sobre o fato de haver investigações e os seus resultados. Auxilia no processo de legitimação da organização, pois explicita que há uma ação estatal além de deixar claro os critérios utilizados. Adicionalmente, fica evidente quando há reincidência, o que impacta tanto no processo interno da organização, quanto na no nível de confiança dos titulares.

Conclusões e caminhos para a ANPD:

Ante as razões expostas, sugere-se como norte **procedimentos explicativos, básicos e intuitivos para o público.** São pilares fundamentais para um sistema eficiente e, consequentemente, mais êxito para o papel da autoridade perante os titulares e controladores.

Igualmente, a resposta ante os controladores não deve ser uma lista fixa e exaustiva de medidas a serem adotadas, mas deve-se trabalhar dentre as diferentes possibilidades com recomendações pontuais, vez que diferentes tipos de incidentes vão exigir diferentes medidas. As diretrizes do EDPB, (Guidelines 01/2021) apontam para isso.

O decorrer do tempo permitirá a criação de procedimentos e indicações de medidas com certo grau de padronização, baseados em uma espécie de jurisprudência ou casos padrão. Nesse momento, pode-se ter mais claramente indicações de providências específicas. Antes de alcançar tal estado, corre-se o risco de ser insuficiente ou excessivo nas abordagens tomadas. Não sendo eficiente, ou desperdiçando energia que poderia ser melhor empregada em questões mais emergenciais.

Portanto, **cabe dimensionar os procedimentos e compreender a função da autoridade em seus aspectos de atuação como plataforma e como serviço em que possa servir como coordenadora, intermediária e facilitadora da resolução de incidentes de segurança.**

2. QUANDO UM INCIDENTE PODE ACARRETAR RISCO OU DANO RELEVANTE AO TITULAR? QUAIS CRITÉRIOS DEVEM SER CONSIDERADOS PELA ANPD PARA AVALIAR O RISCO OU DANO COMO RELEVANTE?

O conceito de de “risco ou dano relevante ao titular” aparece na Lei Geral de Proteção de Dados (LGPD) no art. 48, ao disciplinar a necessidade de comunicação pelo controlador tanto ao titular dos dados quanto à Autoridade Nacional de Proteção de Dados (ANPD) sobre a ocorrência de incidente de segurança. Estabelece um critério de relevância (do risco ou do dano) e um pessoal (ao titular) para haver uma comunicação.

Nesse contexto, cabe construir limites claros que permitam distinguir incidentes de segurança que possam trazer risco ou dano relevante e, por tal razão, demandem providências específicas. A lógica da lei foi no sentido de discriminar situações que merecem maior cuidado e atenção das que não merecem para evitar tanto sobrecarregar a autoridade como não gerar “fadiga de notificações”.

No intuito de alcançar tal discrimnação, é importante ter em vista as experiências internacionais para poder identificar (i) como são classificados incidentes de segurança em outras localidades; e (ii) quais são os parâmetros balizadores utilizados.

UNIÃO EUROPÉIA

» Quando um incidente pode acarretar risco ou dano relevante ao titular?

O General Data Protection Law (GDPR) define seu 'personal data breach' no Artigo 4(12) como *"violação de segurança levando à destruição acidental ou ilegal, perda, alteração, não autorizada divulgação ou acesso a dados pessoais transmitidos, armazenados ou processados de outra forma".*

Nos termos do Artigo 33(1), considera que um incidente de segurança que envolve dados pessoais deve ser notificado à autoridade competente, salvo quando é improvável resultar em um risco a direitos e liberdades das pessoas naturais. Em sequência, a regra para a notificação aos titulares, preconizada no Artigo 34(1), estabelece que o incidente será comunicado quando acarretar um alto risco para os direitos e liberdades de pessoas naturais.

O Considerando 75 oferece contornos ao que constituiria um risco a direitos e liberdades de pessoas naturais. Nesse sentido, o risco para os direitos e liberdades pode resultar do processamento de dados pessoais que levem a danos físicos, materiais ou imateriais aos indivíduos cujos dados foram violados. A título exemplificativo, tais danos são discriminação, roubo de identifdade ou fraude, perdas financeiras e danos à reputação, perda de controle sobre os dados pessoais, limitação de direitos, entre outros. Quando o incidente envolver dados pessoais que revelam racismo origem étnica, opinião política, religião, crenças filosóficas, filiação a sindicatos, dados genéticos, dados relativos à saúde ou à vida sexual, condenações criminais ou medidas de seguranças relacionais, tais danos devem ser considerados prováveis de ocorrer. (Ver Considerando 75 e 85 para mais informações).

» Critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante.

O Considerando 76 aponta que a probabilidade e gravidade do risco para os direitos e liberdades do titular dos dados devem ser determinadas por referência à **natureza, escopo, contexto e objetivos do tratamento.** O risco deve ser mensurado com base em uma avaliação objetiva, pela qual é estabelecido se as operações de processamento de dados envolvem um risco ou um alto risco.

A General Data Protection Law (GDPR) em seu Artigo 35(3) exemplifica quando o processamento de dados pode acarretar risco alto aos titulares, quais sejam: *"a) uma avaliação sistemática e extensa dos aspectos pessoais relativos às*

pessoas físicas que se baseia em processamento automatizado, incluindo criação de perfil, e nas quais as decisões são que produzam efeitos jurídicos em relação à pessoa singular ou afetem de forma significativa a pessoa natural; b) tratamento em grande escala de categorias especiais de dados referidos no Artigo 9(1), ou de dados pessoais relativos a condenações criminais e infrações referidas no Artigo 10; c) um acompanhamento sistemático de uma área acessível ao público em grande escala."

Ante um incidente que resulte em alto risco aos titulares, o Considerando 84 exige que seja realizada uma avaliação de risco e impacto (DPIA). Os critérios a serem considerados nesta são:

I. **Avaliação ou pontuação,** incluindo criação de perfil e previsão, especialmente de "aspectos relativos ao desempenho do titular dos dados no trabalho, situação econômica, saúde, preferências pessoais ou interesses, fiabilidade ou comportamento, localização ou movimentos". (Considerandos 71 e 91).

II. **Tomada de decisão automatizada** com efeito legal ou similar significativo: processamento que visa tomar decisões sobre os titulares dos dados que produzam "efeitos jurídicos relativos à pessoa singular" ou que "afeta de forma significativa de forma semelhante a pessoa singular" (Artigo 35 (3) (a)).

III. **Monitoramento sistemático:** processamento usado para observar, monitorar ou controlar os titulares dos dados, incluindo dados coletados por meio de "um monitoramento sistemático de uma área acessível ao público" (Artigo 35 (3) (c)).

IV. **Dados sensíveis:** incluem categorias especiais de dados (por exemplo informações sobre opiniões políticas de indivíduos), bem como dados pessoais relacionados a crimes, condenações ou ofensas.

V. **Dados processados em grande escala:** o GDPR não define o que constitui grande escala, embora o Considerando 91 forneça algumas orientações. O WP29 recomenda que sejam considerados (i) o número de titulares de dados envolvidos; (ii) o volume de dados e/ou a gama de diferentes itens de dados sendo processados; (iii) a duração, ou permanência, da atividade de processamento de dados; (iv) a extensão geográfica da atividade de processamento

VI. **Conjuntos de dados que foram combinados,** por exemplo, originado de dois ou mais dados operações de processamento realizadas para diferentes fins e/ou por diferentes controladores de dados de forma a exceder as expectativas razoáveis do titular dos dados.

VII. **Dados relativos a titulares de dados vulneráveis** (Considerando 75): o tratamento deste tipo de dados pode exigir um DPIA devido ao aumento do desequilíbrio entre o titular dos dados e o controlador de dados, isso significa que o indivíduo pode ser incapaz de consentir ou se opor ao processamento de seus dados

VIII. Uso inovador ou aplicação de soluções tecnológicas ou organizacionais, como combinar o uso de impressão digital e reconhecimento facial para melhor controle de acesso físico, dentre outras.

IX. Transferência de dados através das fronteiras fora da União Europeia (Considerando 116).

Quando o processamento em si **"impede que os titulares dos dados exerçam um direito ou usem um serviço ou contrato"**(Artigo 22 e Considerando 91).

A *Working Party* ("WP29") considera que quanto mais critérios forem atendidos pelo processamento, maior será a probabilidade de apresentar um alto risco para os direitos e liberdades dos titulares dos dados.

REINO UNIDO

O Reino Unido utiliza critérios semelhantes à União Europeia para a definição de incidentes de segurança relacionados a dados pessoais. Encontra-se, no entanto, diferentes ferramentas para auxiliar as organizações a conduzirem a avaliação dos incidentes.

Nesse sentido, a ICO (*Information Commissioner's Office*) apresenta um "quiz" de aproximadamente cinco minutos para verificar a probabilidade e gravidade do risco aos direitos e liberdades das pessoas, após a violação, bem como a necessidade de notificar a ICO. Caso ainda restem dúvidas, pode-se recorrer ao *Data Security and Protection Incident Reporting tool*, que reúne diversos documentos e relatórios sobre incidentes de segurança.

Destes se depreende dois pontos de análise: a seriedade do impacto eventual (ou atual) e a probabilidade de o impacto ocorrer. Tanto maior é o risco - que merece notificação - se houver maior severidade de um impacto e da probabilidade de que este ocorra. *Dois exemplos utilizados* pela ICO podem explicitar a situação:

- Histórico de pacientes de um hospital vazaram. Aqui há potencial impacto alto pela natureza de saúde dos dados. O que deve levar a um risco elevado.
- Dados de um paciente foram enviados de um médico a outro sem autorização de maneira acidental. Providências foram tomadas e houve a exclusão dos dados pelo segundo médico. Ainda que houvesse o mesmo potencial de impacto, devido a mesma natureza de saúde dos dados, o fato de que há uma probabilidade baixa de o impacto efetivamente ocorrer, faz com que se entenda que o risco seria mais baixo.

Nesse contexto parece existir uma matriz em que severidade e probabilidade podem se cruzar. E o resultado dessa intersecção é que determina o risco.

CANADÁ

» Quando um incidente pode acarretar risco ou dano relevante ao titular.

De forma semelhante à LGPD, a legislação de proteção de dados do Canadá *Personal Information Protection and Electronic Documents Act* (PIPEDA) exige que organizações reportem à autoridade de supervisão canadense quando incidentes de segurança envolverem dados pessoais que acarretem risco real de dano relevante aos indivíduos.

Nos termos da legislação, dano relevante significaria danos corporais, humilhação, danos à reputação ou relacionamentos, perda de emprego, oportunidades de negócios ou profissionais, perda financeira, roubo de identidade, efeitos negativos no registro de crédito e danos ou perda de propriedade.

De acordo com a autoridade nacional de proteção de dados canadense, a avaliação para verificar risco de dano relevante deve considerar a **sensibilidade das informações envolvidas e a probabilidade de que as informações sejam mal utilizadas.**

» Critérios devem ser considerados pela ANPD para avaliar o risco ou dano como relevante.

No que tange aos critérios, a lei Canadense foca na **sensibilidade** dos dados e na **probabilidade que sejam mal utilizados.** Entende que estes dois pontos norteadores para avaliação se o risco de dano deve ser considerado como relevante. Nesse sentido, deve-se considerar os critérios a serem analisados nesses dois pontos norteadores.

No contexto da legislação canadense, o Princípio 4.3.4 da PIPEDA auxilia na explicitação deste ponto quando expõe que "(...) *apesar de algumas informações (por exemplo, registros médicos e registros de receita) serem quase sempre consideradas sensíveis, qualquer informação pode ser sensível, dependendo do contexto. Por exemplo, os nomes e endereços dos assinantes de uma revista de notícias geralmente não são considerados informações sensíveis. No entanto, os nomes e endereços dos assinantes de algumas revistas de interesse especial podem ser considerados sensíveis.*"

Dessa forma, na análise de um incidente, não só a natureza dos dados pessoais presentes deve ser avaliada, como também deve ser cotejada com o contexto em que se encontram os dados. As circunstâncias do incidente podem tornar as informações sensíveis além de poder impactar os danos em potencial.

No que tange a possibilidade de **mal uso dos dados**, a autoridade canadensa elenca diversas questões a serem consideradas, dentre elas: qual a probabilidade de alguém ser prejudicado pelo incidente? Quem realmente acessou ou pode-

ria ter acessado os dados pessoais? Há quanto tempo os dados pessoais foram expostos? Há evidências de intenção maliciosa (por exemplo, roubo, hacking)? A informação foi perdida, acessada indevidamente ou roubada? Os dados pessoais foram recuperados? Os dados pessoais estão adequadamente criptografados, anonimizados ou não são facilmente acessíveis?

Conclusões e caminhos para a ANPD:

A partir da análise do contexto europeu em conjunto ao canadense, nota-se determinada divergência entre as definições para incidentes de segurança e, por conseguinte, as interpretações acerca de quando um incidente pode acarretar risco ou dano também detém particularidades.

De forma geral, a União Européia e o Reino Unido consideram que o incidente que viola dados pessoais deve ser reportado à autoridade via de regra, salvo quando é improvável resultar em risco à direitos e liberdades. Por sua vez, na legislação do canadense, deve-se reportar o incidente de segurança quando existem circunstâncias razoáveis para deduzir que houve risco real de dano relevante.

A lógica do texto da lei brasileira, ainda que muito inspirada na europeia, parece estar mais próxima do sistema canadense no sentido de entender que risco e dano são elementos diferentes e que a notificação deve ocorrer em casos em que exista risco ou mesmo em que exista dando. O que leva a crer que a análise de risco deve ser separada da análise do potencial de dano.

O risco deve ser, então, entendido de maneira mais ampla contemplando restrições a liberdades que ainda que não causem danos quantificáveis também devem ser reportadas.

Não seria nem qualquer risco e nem qualquer dano que deve ter como consequência a notificação. Nesse contexto, entende-se que em paralelo deva existir uma análise de se o risco é relevante e se o dano é relevante.

Os critérios em si que permitem compreender a relevância parecem ser similares e se referem a sensibilidade do dado, extensão do incidente. O que muda é a potencialidade de materialização do risco a direitos e liberdades ou de danos.

Nesse sentido, a sugestão é a realização de análises paralelas da relevância do risco e após do dano.

3. O RISCO OU DANO RELEVANTE DEVERIA SER SUBDIVIDIDO EM MAIS CATEGORIAS (EX. BAIXO, MÉDIO, ALTO, ETC)? COMO DISTINGUIR OS NÍVEIS?

No intuito de traçar mais contornos aos incidentes de segurança, cabe comentar sobre a possibilidade de subdividi-los em categorias. Com base nas experiências internacionais, a **subdivisão parece permitir às autoridades a direcionarem esforços e medidas cabíveis a cada tipo de incidente.**

UNIÃO EUROPÉIA

A conceituação de risco na União Europeia advém de um quadro já presente nos considerandos ("recitals") do GDPR. Nesse sentido, o Considerando 76 indica que a probabilidade e a gravidade do risco para os direitos e liberdades do titular dos dados devem ser determinadas por referência à natureza, âmbito, contexto e objetivos do tratamento. O risco deve ser avaliado com base em uma avaliação objetiva, pela qual é estabelecido se as operações de processamento acarretam nenhum risco, risco ou alto risco.

Cumpre ressaltar que o Considerando 75 do GPDR, ao trazer especificações sobre os riscos à direitos e liberdades das pessoas naturais, destaca a variação de a possibilidade e gravidade entre eles. Isto posto, denota a importância de classificar em diferentes níveis os riscos também para atender com mais eficácia violações mais severas aos direitos e liberdades.

Ao tratar de **riscos elevados**, o artigo 35(3) fornece exemplos e o Guia para Avaliação de Impacto de Proteção de Dados da WP29 indica 10 diretrizes a serem consideradas, bem como exemplos concretos para sua avaliação. De acordo com o documento, como regra geral, operações de tratamento que satisfaçam menos de dois critérios são consideradas de menor nível de risco, enquanto ao satisfazer pelo menos dois desses critérios são consideradas de alto risco.

Nesse diapasão, as *Guidelines on Personal Data Breach Notification under Regulation 2016/679* recomendam que circunstâncias específicas de incidente devam ser consideradas para avaliar o risco aos indivíduos após uma violação, incluindo a gravidade do dano potencial e probabilidade do dano ocorrer. Quando as consequências de uma violação forem mais graves, o risco é maior e da mesma forma, onde a probabilidade de ocorrerem é maior, o risco também é aumentado. Assim, poder-se-ia utilizar tais critérios para distinguir os níveis de risco. Sejam eles:

I. **Tipo de violação:** O tipo de violação ocorrida aos dados pessoais pode afetar o nível de risco apresentado aos indivíduos. Por exemplo, uma violação de sigilo em que informações médicas foram divulgadas a pessoas não autorizadas pode resultar em diferentes consequências ao indivíduo, se comparada a uma violação em que detalhes médicos foram perdidos e não

estão mais disponíveis.

II. Natureza, sensibilidade e volume dos dados pessoais: No processo de avaliação do risco ou dano como relevante, a natureza, sensibilidade e volume de dados pessoais comprometidos pelo incidente de segurança é fundamental. Quanto mais sensíveis os dados, maior será o risco de danos às pessoas afetadas, mas deve-se levar em consideração outros dados pessoais que já podem estar disponíveis sobre o titular dos dados. Incidentes envolvendo dados de saúde, documentos de identidade ou dados financeiros, como detalhes de cartão de crédito, causam danos por si próprios, mas se juntos, podem ser usados para roubo de identidade. Uma combinação de dados pessoais é normalmente mais sensível do que um único pedaço de dados pessoais.

III. Facilidade de identificação de indivíduos: A depender das circunstâncias, a identificação pode ser possível diretamente a partir dos dados comprometidos, sem buscas adicionais, enquanto em outros casos, pode ser mais difícil de combinar o dado pessoal a um indivíduo em particular.

IV. Gravidade das consequências para os indivíduos: Dependendo da natureza dos dados pessoais envolvidos em um incidente de segurança, por exemplo, categorias especiais de dados, o dano potencial aos indivíduos que poderia resultar pode ser especialmente grave, em particular onde a violação resultar em roubo de identidade ou fraude, dano físico, sofrimento psicológico, humilhação ou danos à reputação. Se a violação envolver dados pessoais sobre indivíduos vulneráveis, o risco de dano é ainda maior. Por outro lado, quando dados são divulgados a terceiros não autorizados acidentalmente e o controlador possuir um nível de confiança com o destinatário de modo a possibilitar certa expectativa de cooperação, a gravidade do incidente pode ser erradicada. Deve-se considerar também a permanência das consequências para os indivíduos, onde o impacto é visto como maior se os efeitos forem de longo prazo.

V. Características especiais do indivíduo: Quando um incidente afeta dados pessoais relativos a crianças ou outros indivíduos vulneráveis pode ser considerado de maior risco de dano.

VI. Características especiais do controlador de dados: A natureza e o papel do controlador e suas atividades podem impactar o nível de risco para os indivíduos envolvidos no incidente. Uma organização médica irá processar categorias especiais de pessoal dados, portanto, há uma ameaça maior para os indivíduos se seus dados pessoais forem violados.

VII. Número de indivíduos afetados: Geralmente, quanto maior o número de indivíduos afetados, maior o impacto de uma violação.

Na União Europeia, portanto, a graduação dos riscos é dependente de fatores intrínsecos e extrínsecos aos dados, impactando quanto mais os fatores no nível de risco específico. Quanto maior os riscos, maior o mérito em realizar a notifi-

cação e tomar providências o mais rápido possível. Sendo necessário por vezes envolver diferentes atores (controladores e indivíduos são o ponto de partida).

REINO UNIDO

No Reino Unido, o *Guide to the Notification of Data Security and Protection Incidents* apresenta formas de subdivisão dos incidentes de segurança. Nesse sentido, o incidente deve ser classificado de acordo com o impacto no indivíduo ou grupos de indivíduos e não na organização. O grau da relevância e a probabilidade de ocorrência das consequências podem ser medidos em escala de 1 a 5. Nesse sentido, como comentamos acima na resposta anterior, segue uma lógica matricial de severidade e probabilidade.

Por exemplo, quando o incidente está relacionado a um grupo vulnerável a pontuação mínima será 2 em relevância ou probabilidade, a menos que o incidente tenha sido contido. Nos exemplos mencionados na pergunta anterior, o caso em que foram tomadas medidas rápidas fez com que diminuísse a probabilidade da consequência adversa - ainda que a seriedade do impacto pudesse ainda ser a mesma.

Para estabelecer a probabilidade de que o efeito adverso mediante o incidente, deve-se analisar:

- Nível 1: Há uma certeza absoluta de que pode haver nenhum efeito adverso.
- Nível 2: Nos casos em que não há evidências que possam provar que nenhum efeito adverso ocorreu.
- Nível 3: É provável que haja um efeito adverso decorrentes da violação.
- Nível 4: Há quase certeza de que em determinado momento um efeito adverso acontecerá.
- Nível 5: Há uma ocorrência relatada de um efeito adverso decorrente do incidente de segurança.

Conclusões e caminhos para a ANPD:

Dentro da mesma lógica da experiência internacional, parece ser útil a modulação em níveis para distinguir os tipos de ações tanto da própria ANPD como dos controladores.

Dentro de conceitos de governo como plataforma e como serviço, é relevante poder classificar de maneira diferentes os incidentes vis-à-vis o seu impacto e complexidade. Uma chave para realizar essa classificação e as consequentes ações que daí decorrerão é partir da própria concepção legislativa e subdividir em diferentes níveis tanto de risco como de dano. Os critérios utilizados pela União Europeia a partir do GDPR são um bom indicativo de referência: (i) tipo de violação; (ii) natureza, sensibilidade e volume dos dados pessoais; (iii) facilidade de identificação de indivíduos; (iv) gravidade das consequências para os indivíduos; (v) características especiais do indivíduo; (vi) características especiais do controlador de dados; (vii) número de indivíduos afetados.

Já a lógica matricial utilizada pela ICO no Reino Unido prevê um mecanismo procedimental para realizar a análise. O que em um futuro próximo, se for esse o caminho seguido pela ANPD, poderia valer a criação de uma ferramenta tecnológica que facilitasse essa análise de risco e dano.

Essas diferentes subdivisões de risco e dano facilitaram a compreensão de como agir de acordo com os preceitos legais, o que vai além das obrigações de notificação. Incluem também mecanismos de segurança, de lida com danos e resiliência.

4. QUAIS SÃO OS POSSÍVEIS CRITÉRIOS A SEREM ADOTADOS PELA ANPD NA ANÁLISE DA GRAVIDADE DO INCIDENTE DE SEGURANÇA? (ART. 48, §2º)

Após um incidente, é importante examinar quais dados pessoais foram violados e as circunstâncias de sua ocorrência. As circunstâncias do incidente podem tornar as informações mais ou menos confidenciais. Os danos potenciais que podem advir para um indivíduo também são um fator importante.

UNIÃO EUROPEIA:

Os critérios apontados no documento *Guidelines on Personal Data Breach Notification under Regulation 2016/679* e elencados anteriormente podem servir de inspiração para os critérios a serem adotados pela ANPD para análise da gravidade do incidente de segurança.

Além disso, com base em um estudo da Agência Europeia para a Segurança das Redes e da Informação (ENISA) de 2011 sobre a implementação do Artigo 4 da Diretiva de Privacidade Eletrônica, as Autoridades de Proteção de Dados da Grécia e da Alemanha, em colaboração com a ENISA, desenvolveram uma metodologia para avaliação da gravidade da violação de dados que poderia ser usada tanto pelas autoridades de proteção de dados quanto pelos controladores de dados.

De acordo com a metodologia, os principais critérios levados em consideração ao avaliar a gravidade de uma violação de dados pessoais são:

a) Contexto de processamento de dados (CPD): aborda o tipo de dados violados, juntamente com um vários fatores ligados ao contexto geral de processamento.
b) Facilidade de Identificação (FI): Determina a facilidade com que a identidade dos indivíduos pode ser deduzida dos dados envolvidos na violação.
c) Circunstâncias de violação (CV): Aborda as circunstâncias específicas da violação, que são relacionadas ao tipo de violação, incluindo principalmente a perda de segurança dos dados violados, bem como qualquer intenção maliciosa envolvida.

Conclusões e caminhos da ANPD:

A visão internacional sobre como lidar com incidentes de segurança entende que a gravidade depende dos seguintes critérios: (i) contexto de processamento de dados; (ii) facilidade de Identificação; (iii) circunstâncias de violação. Quanto à metodologia, detalha-se abaixo.

5. EXISTE ALGUMA METODOLOGIA RECOMENDADA PARA A ANÁLISE DE GRAVIDADE DO INCIDENTE DE SEGURANÇA? SE SIM, QUAL(IS)?

A metodologia para análise de gravidade do incidente de segurança é importante na busca de padronizar sua implementação e auxiliar organizações a se auto-avaliarem.

UNIÃO EUROPEIA:

A Agência da União Europeia para a Segurança das Redes e da Informação (ENISA), em colaboração com as Autoridades de Proteção de Dados da Grécia e Alemanha, produziram recomendações para uma metodologia de avaliação da gravidade do incidente de segurança. O relatório pode ser utilizado por controladores e processadores ao projetarem seu plano de resposta de gerenciamento ao incidente de segurança.

A metodologia proposta é baseada em uma abordagem objetiva, matricial, sendo flexível o suficiente para ser adotada por várias autoridades de proteção de dados, ajustando-se ao tamanho, e ao sistema jurídico nacional.

No contexto da metodologia indicada, a gravidade do incidente de segurança envolvendo dados pessoais é definida como "*estimativa da magnitude do impacto potencial sobre os indivíduos derivada dos dados violados*". São indicados três critérios principais para avaliar a gravidade do incidente (já descritos acima, mas por facilitação repetidos aqui), quais sejam eles:

a) Contexto de processamento de dados (*Data Processing Context DPC*): endereça o tipo de dados violados, juntamente com um vários fatores ligados ao contexto geral de processamento. Para definir a pontuação deste critério, deve-se (i) definir e classificar os tipos de dados pessoais, de forma a definir os dados envolvidos no incidente e categorizá-los em quatro (simples, comportamentais, financeiros e sensíveis); (ii) estabelecer quais fatos contextuais podem aumentar ou reduzir a pontuação, como volume de dados e natureza.
b) Facilidade de identificação (*Ease of Identification EI*): determina a facilidade com que a identidade dos indivíduos pode ser deduzida dos dados envolvidos na violação. Para essa metodologia, esse critério

pode ser definido em quatro níveis: insignificante, limitado, significativo e máximo. A pontuação mais baixa é dada quando a possibilidade de identificar o indivíduo é insignificante e a mais alta quando é possível identificar diretamente a partir dos dados violados.

c) Circunstâncias do incidente (*Circumstances of breach CB*): endereça as circunstâncias específicas da violação, que são relacionadas ao tipo de violação, incluindo principalmente a perda de segurança dos dados violados, bem como qualquer intenção maliciosa envolvida. São quatro os elementos a serem considerados: confidencialidade, integridade, disponibilidade e intenção maliciosa.

Com base nesses critérios, tem-se: a) o contexto de processamento de dados está no centro da metodologia e serve como avaliador da criticalidade de determinado conjunto de dados para um processamento específico; b) a facilidade de identificação pode reduzir a criticidade geral de um processamento de dados. Dessa forma, com a combinação desses dois elementos iniciais se obtém a 'pontuação' inicial do incidente de segurança ("SE"); c) as circunstâncias do incidente podem estar presente ou não em uma situação específica, esse fator pode aumentar a severidade do incidente.

Como resultado, metodologia específica para o cálculo do risco seria: "*DPC x EI + CB*", ou seja, combinar o contexto de processamento de dados com a facilidade de identificação, incluindo então as circunstâncias do incidente. Ao final, a gravidade do incidente é categorizada em baixo, médio, alto e muito alto a partir do cálculo realizado.

A lógica pensada segue em parte a compreensão matricial do risco para o titular somente com elementos de agregação específicos para representar a coletividade do incidente de segurança.

Conclusões e caminhos da ANPD:

Como visto, o uso de metodologia específica auxilia as autoridades a avaliarem a gravidade e complexidade de um incidente. É indicado que a definição dos critérios apresentados seja pensada no contexto brasileiro, considerando as legislações internas pertinentes e apresentada de forma clara aos controladores. A proposta seria enviar também a avaliação e metodologia adotadas pela autoridade aos controladores no formulário de notificação ou mesmo incluída por meio de quiz com perguntas e exemplos.

6. QUAIS INFORMAÇÕES OS CONTROLADORES DEVEM NOTIFICAR À ANPD, ALÉM DAQUELAS JÁ LISTADAS NO §1º DO ART. 48?

Tendo em vista a inspiração da Lei Geral de Proteção de Dados (LGPD) nos diferentes modelos internacionais, nota-se que já há uma base significativa quanto aos elementos já listados no §1º do art. 48.

O que se buscará mais adiante é apresentar o que pode ser incluído com inspiração nas demais legislações e em como as autoridades regulamentaram suas regras. Ao final, serão aduzidas recomendações objetivas a respeito do que seria relevante replicar das demais práticas.

UNIÃO EUROPÉIA

A maioria das informações que os controladores devem notificar à ANPD, listadas no §1º do art. 48 da LGPD estão refletidas na GPDR. Cabe, contudo, detalhar as diferenças e considerações do WP29 referente ao tema.

Nos termos do art. 48, §1º, I e II da LGPD, é necessário descrever a natureza dos dados pessoais afetados e as informações sobre os titulares envolvidos. O comando equivalente na legislação europeia exige também que **tal informação esteja acompanhada, sempre que possível, das categorias e número aproximado de titulares (Artigo 33 (A)).**

Como GDPR é silente sobre quais seriam as categorias de titulares de dados ou registros de dados pessoais, WP29 sugere categorias de titulares de dados para se referir aos vários tipos de indivíduos cujos dados pessoais foi afetado por uma violação, por exemplo, crianças e outros grupos vulneráveis, pessoas com deficiência, funcionários ou clientes. Similarmente, **categorias de registros de dados pessoais** podem se referir aos diferentes tipos de registros que o controlador pode processar, como dados de saúde, registros educacionais, informações de assistência social, detalhes financeiros ou bancários, números de passaporte e assim por diante.

No mesmo sentido, o Considerando 85 deixa claro que um dos objetivos da notificação é a limitação dos danos às pessoas. Consequentemente, se os tipos de titulares de dados ou os tipos de dados pessoais indicarem um risco de dano ocorrido como resultado do incidente (por exemplo, roubo de identidade, fraude, perda financeira, ameaça ao sigilo profissional), é importante que a notificação indique essas categorias.

Além disso, exige-se também o nome e os detalhes de contato do responsável pela proteção de dados ou outro ponto de contato onde mais informações podem ser obtidas.

A legislação europeia ressalta ainda a necessidade das organizações manterem um registro dos incidentes de segurança relacionados a dados

pessoais. Essa documentação permitirá à autoridade de supervisão verificar a conformidade com a legislação de proteção de dados, compreender eventuais incidentes futuros e, ainda, auxiliar em caso de reincidência.

REINO UNIDO

A autoridade de proteção de dados do Reino Unido indica a necessidade de fornecer: nome e detalhes de contato; data e hora da violação (ou uma estimativa); data e hora em que o incidente foi detectado; informações básicas sobre o tipo de violação; e informações básicas sobre os dados pessoais em questão.

Ainda, requer, se possível, a inclusão de detalhes completos do incidente, o número de indivíduos afetados e os possíveis efeitos sobre eles, as medidas tomadas para mitigar esses efeitos e informações sobre a notificação aos titulares. Caso tais detalhes não estejam disponíveis, deve-se enviar um segundo formulário de notificação em três dias com tais detalhes ou informando quanto tempo levará para enviá-los.

CANADÁ

Em regulação específica, o Canadá estabelece os processos relativos às salvaguardas de incidentes de segurança (*Breach of Security Safeguards Regulations: SOR/2018-64*). De acordo com a normativa, a notificação do incidente à autoridade competente deve conter, dentre outros elementos: i. descrição das circunstâncias do incidente, caso a causa seja conhecida; ii. data ou o período durante o qual, a violação ocorreu ou, se nenhum for conhecido, o período aproximado; iii. o número de indivíduos afetados, caso desconhecido, o número aproximado; iv. descrição das etapas que a organização tomou ou pretende realizar para notificar os indivíduos afetados; v. o nome e contato de quem possa responder, em nome da organização, às perguntas da autoridade.

Ainda, abre-se a possibilidade para que a organização submeta informações novas relacionadas ao incidente, caso fique ciente após notificação à autoridade.

Conclusão e caminhos para ANPD:

Com base nas melhores práticas internacionais e no intuito de complementar as informações exigidas no §1º do art. 48 da LGPD, recomenda-se que controladores também forneçam:

I. Nome e contato do Encarregado ou outro ponto de contato na instituição.

II. Data ou o período durante o qual, o incidente ocorreu ou, se nenhum for conhecido, o período aproximado;

III. Detalhes complementares sobre a natureza dos dados pessoais afetados e as informações sobre os titulares envolvidos, quais sejam: as categorias e número aproximado de titulares;

IV. Etapas que a organização tomou ou pretende realizar para notificar os indivíduos afetados, quando necessário por lei ou por prudência;

V. Registro de incidentes de segurança, incluindo os fatos relacionados à violação, efeitos e as medidas corretivas tomadas.

Há que se ter em mente que apesar de ser necessário o procedimento seguir uma lógica de formulário e ser estruturado, deve existir certa flexibilidade. Não só as mudanças tecnológicas podem afetar os incidentes, como podem existir fatores inesperados e deve haver campos e espaços abertos para poder lidar com essa aleatoriedade.

7. QUAL O PRAZO RAZOÁVEL PARA QUE CONTROLADORES INFORMEM A ANPD SOBRE O INCIDENTE DE SEGURANÇA? (ART. 48, §1º)

Como já demonstrado, um incidente de segurança pode acarretar uma série de efeitos adversos significativos sobre os indivíduos, que podem representar danos físicos, materiais ou imateriais. A prontidão na notificação do incidente à ANPD detém relação direta com a gravidade do dano acarretado ao titular, por isso é importante tratar do tema com a devida cautela.

Sabe-se que atualmente o Decreto 9.936/2019, que regulamenta a Lei do Cadastro Positivo, exige que a comunicação à ANPD seja efetuado no prazo de dois dias úteis (art. 18, I e §§ 1º e 2º). Ainda, a orientação atual também é no sentido de que caso não seja possível fornecer todas as informações no momento da comunicação preliminar, informações adicionais poderão ser fornecidas posteriormente.

De todo modo, busca-se expor os parâmetros internacionais tanto a respeito do prazo para comunicação dos incidentes como recomendar que seja estabelecido prazo para as informações adicionais essenciais, com base nas práticas internacionais.

Como se observará adiante, o prazo comum é de no máximo 72 horas após ciência e, na hipótese de informações, deve-se explicar o atraso e quando pode ser esperado o envio dos detalhes adicionais.

» Qual o prazo razoável para que controladores informem a ANPD sobre o incidente de segurança? (art. 48, §1º)

UNIÃO EUROPÉIA

A legislação europeia estabelece o prazo de 72 horas para a notificação do incidente de segurança. Conforme o Artigo 33(1) do GDPR, na hipótese de violação de dados pessoais, o controlador deve, sem demora indevida e, quando viável, sob o prazo máximo de 72 horas após ciência, notificar o incidente de segurança à autoridade supervisora de proteção de dados. Salvo casos em que

seja improvável que o incidente resulte em risco para os direitos e liberdades das pessoas singulares. Quando a notificação para a autoridade é feita após o prazo de 72 horas, deve ser acompanhada dos motivos do atraso.

De acordo com o WP29, a ciência do controlador a respeito do incidente de segurança se dá mediante um grau razoável de certeza de que ocorreu um incidente a comprometer dados pessoais. Isso pode variar a depender das circunstâncias específicas do incidente. Em alguns casos, será relativamente claro desde o início que houve uma violação, enquanto em outros, pode levar algum tempo para estabelecer se os dados pessoais foram comprometidos. No entanto, a ênfase deve ser na ação imediata para investigar um incidente para determinar se os dados pessoais foram realmente violados e, em caso afirmativo, tomar medidas corretivas e notificar se necessário

Na hipótese de controladores conjuntos, o Artigo 26 do GDPR preconiza a necessidade dos controladores determinarem suas respectivas responsabilidades pelo cumprimento do GDPR. O WP29 recomenda que os acordos contratuais entre controladores conjuntos incluam disposições que determinam quais o controlador assumirá a liderança ou será responsável pela conformidade com a notificação de incidentes de segurança, nos termos do GDPR.

REINO UNIDO

Na mesma linha da União Européia, a GDPR do Reino Unido (UK GDRP) impõe a todas as organizações o dever de relatar certas violações de dados pessoais à autoridade supervisora relevante. A notificação deve ser feita dentro de 72 horas após tomar conhecimento dos fatos essenciais da violação, quando viável.

É esperado que os controladores priorizem a investigação, empregando os recursos adequados com a devida urgência. No caso de ultrapassar o prazo de 72 horas, é recomendado explicar o porquê e indicar uma expectativa de envio futuro.

Conclusões e caminhos para a ANPD:

De um ponto de vista da experiência europeia, tem-se que 72 horas da ciência é o prazo prudencial. Nada parece levar a que no sistema estabelecido na LGPD o prazo razoável deva ser menor do que este prudencial encontrado no sistema europeu. Frise-se que não é o prazo mínimo, mas o máximo. A prontidão na notificação deve ser exaltada.

Nesse diapasão, a ANPD deve incentivar a notificação oportuna. O que não quer necessariamente dizer antecipada. É importante para a atuação adequada da autoridade que sejam fornecidas informações suficientes para permitir a procedimentalização correta das ações, seja da autoridade enquanto plataforma, seja enquanto serviços.

Este prazo deve ser entendido no sentido de incentivar uma atuação de boa-fé por parte dos controladores. Há um espaço de tomada de decisão e de atuação imediata do controlador. O que se espera é a existência das mais prontas medidas de mitigação e de resiliência.

8. QUAL SERIA UM PRAZO RAZOÁVEL PARA QUE OS CONTROLADORES INFORMEM OS TITULARES DE DADOS SOBRE O INCIDENTE DE SEGURANÇA? (ART. 48, §1º) QUAIS INFORMAÇÕES DEVEM CONSTAR DESSA COMUNICAÇÃO? AS MESMAS DO §1º DO ART. 48?

Assim como o prazo para comunicação à ANPD, o prazo para que os controladores informem aos titulares sobre o incidente de segurança também possui impactos no indivíduo e pode acarretar em efeitos adversos. É o momento de explicar o ocorrido e, caso possível, sugerir providências ou mesmo formas de mitigação de danos que demandem ação da própria pessoa afetada.

Há situações em que a urgência pode ser maior justamente tendo em vista a gravidade, seriedade ou probabilidade de risco ou dano seja mais iminente ou alto. A estrutura de riscos e danos em face da matriz sugerida acima auxilia nessa compreensão e pode recomendar em quais casos é mais premente essa comunicação.

Para sugerir um modelo de resposta preciso, recorreu-se à União Européia, Reino Unido e Canadá, cada um com suas particularidades e focos ao tratar do tema.

UNIÃO EUROPÉIA

» Qual prazo razoável para que os controladores informem os titulares de dados sobre o incidente de segurança?

Em seu Parecer 03/2014 sobre notificação de violação de dados pessoais, o WP29 forneceu orientação aos controladores para ajudá-los a decidir se notificam os titulares dos dados em caso de violação. A manifestação considerou a obrigação dos fornecedores de comunicações eletrónicas no que diz respeito à Diretiva 2002/58/CE, concedeu exemplos de vários setores, no contexto do então rascunho do GDPR, e apresentou boas práticas para todos os controladores.

O GDPR declara que a comunicação de uma violação aos indivíduos deve ser feita “sem indevido atraso”, o que significa o mais rápido possível. O principal objetivo da notificação aos indivíduos é fornecer informações específicas sobre as etapas que devem seguir para sua proteção (Ver Considerando 86).

» Quais informações devem constar dessa comunicação? As mesmas do §1º do art. 48?

A legislação européia em seu Artigo 34(2) especifica a necessidade de a comunicação para os titulares descrever em linguagem clara e simples a natureza da violação de dados pessoais e conter ao menos as informações e medidas referidas nos pontos (b), (c), e (d) do Artigo 33(3), que impõe as informações necessárias durante a notificação da autoridade de supervisão, sejam elas:

a) descrever a natureza da violação;
b) fornecer o nome e os dados de contato do responsável pela proteção de dados ou outro ponto de contato;
c) descrever as consequências (riscos) prováveis da violação; e
d) uma descrição das medidas tomadas ou propostas a serem tomadas pelo controlador para resolver a violação, incluindo, quando apropriado, medidas para mitigar seus possíveis efeitos adversos.

É recomendado ainda que o controlador, quando apropriado, forneça conselhos e auxílio aos titulares sobre como se proteger dos riscos e danos do incidente de segurança, por exemplo, alterar senha no caso de suas credenciais terem sido comprometidas.

REINO UNIDO

» Qual prazo razoável para que os controladores informem os titulares de dados sobre o incidente de segurança?

Ante a possibilidade do incidente resultar em um alto risco para os direitos e liberdades dos indivíduos, o UK GDPR determina que os indivíduos devem ser informados diretamente e sem atrasos indevidos.

» Que informações devem constar dessa comunicação? As mesmas do §1º do art. 48?

A autoridade de supervisão do Reino Unido Information Commissioner Office (ICO) entende que a notificação aos titulares deve conter:

a) Nome e detalhes de contato;
b) Data estimada da violação;
c) Resumo do incidente;
d) Natureza e o conteúdo dos dados pessoais;
e) Efeito provável no indivíduo;
f) Medidas tomadas para resolver a violação;
g) Medidas de mitigação para possíveis impactos adversos.

CANADÁ

Em regulação específica, o Canadá regula os processos relativos às salvaguardas de incidentes de segurança (*Breach of Security Safeguards Regulations: SOR/2018-64*). Nesse sentido, a autoridade estabelece que a notificação aos titulares de dados deve conter:

a) Descrição das circunstâncias da violação;
b) Data ou período durante o qual a violação ocorreu ou, se nenhum for conhecido, o período aproximado;
c) Descrição das informações pessoais que são objeto da violação, na medida em que as informações sejam conhecidas;
d) Descrição das medidas que a organização tomou para reduzir o risco de dano que poderia resultar da violação;
e) Medidas que os indivíduos afetados podem tomar para reduzir o risco de dano que pode resultar da violação ou para mitigar esse dano;
f) Informações de contato que o indivíduo afetado pode usar para obter mais informações sobre a violação.

Conclusões e caminhos para a ANPD:

Percebe-se que diferentemente do prazo para notificação da autoridade, de um modo geral nos sistemas de proteção de dados da Europa e outros países a lógica prudencial predomina. Prazos estritos não necessariamente dão conta da urgência da situação. Há que se ter em mente que a comunicação prematura pode ser também danosa. Uma comunicação sem as informações suficientes pode gerar maior ansiedade.

É importante então que a comunicação seja feita sem demora, mas de uma maneira estruturada e com as informações mínimas necessárias. A lógica da comunicação não é meramente de transparência é de possibilitar uma ação informada pelo titular. Nesse contexto, **a notificação deve vir em um prazo mínimo, de acordo com a urgência e com a informação de maneira completa, acessível e que permita a ação consciente e informada.**

9. 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.)?

A forma de comunicação dos incidentes é mais uma faceta para garantir a mitigação dos danos ocorridos. Com base em experiências de diversos países, nota-se que *inexiste um padrão específico* de comunicação, todavia, a comunicação direta assume posição preferencial nos demais ordenamentos. Nota-se que como visto acima, o objetivo desse tipo de comunicação é mais do que dar transparência ao ocorrido, é também permitir a ação informada e consciente do titular. Para tanto, o formato deve ser subordinado à compreensão fácil do titular, de preferência seguindo cânones de linguagem simples, cidadã ("*plain text*").

No geral, as recomendações são de considerar as particularidades do caso e focar em aumentar a proteção para com relação aos dados violados. Esse aspecto também pesa na relação de confiança entre o titular e o controlador. Passa-se a detalhar as diretrizes internacionais quanto ao tema:

UNIÃO EUROPÉIA

» Qual a forma mais adequada para a realização da comunicação do incidente aos titulares?

Comunicar um incidente aos indivíduos permite que o controlador forneça informações sobre os riscos apresentados como resultado da violação e as medidas que esses indivíduos podem tomar para se protegerem de suas possíveis consequências.

O foco de qualquer plano de resposta a violações deve ser a proteção dos indivíduos e de seus dados pessoais. Consequentemente, a notificação deve ser vista como uma ferramenta para aumentar a conformidade em relação à proteção de pessoas dados.

O WP29 estabelece melhores práticas a serem replicadas ante os diferentes tipos de incidentes:

- **As mensagens de comunicação devem ser movidas exclusivamente para esse fim.** Não se deve enviar outras informações, como atualizações regulares, boletins informativos ou mensagens padrão. O objetivo dessa recomendação é tornar a comunicação do incidente clara e transparente.

- Os controladores também podem precisar garantir que a comunicação seja **acessível em alternativa adequada a formatos e linguagens** relevantes para garantir que os indivíduos sejam capazes de compreender as informações que estão sendo fornecidas.

» A comunicação deve ser sempre direta e individual ou, em determinadas circunstâncias, pode ser admitida a comunicação pública?

Conforme as Guidelines on Personal data breach notification under Regulation do WP29, uma notificação exclusivamente pública, como um comunicado à imprensa ou blog corporativo não seria um meio eficaz de comunicar o incidente de segurança a um indivíduo.

Em síntese, encontra-se as seguintes recomendações sobre como realizar a comunicação com os indivíduos:

- Escolher de um meio que **maximize a chance de comunicar as informações de maneira adequada** a todos os indivíduos afetados.
- Empregar, dependendo das circunstâncias, **vários métodos de comunicação,** em oposição ao uso de um único canal de contato.
- Os controladores estão melhor posicionados para determinar o canal de contato mais apropriado para comunicar uma violação a indivíduos, especialmente se eles interagirem com seus clientes com frequência.

CANADÁ

» A comunicação deve ser sempre direta e individual ou, em determinadas circunstâncias, pode ser admitida a comunicação pública?

No Canadá, admite-se a possibilidade de notificação direta e indireta sob circunstâncias específicas. A notificação direta deve ser dada ao indivíduo afetado pessoalmente, por telefone, correio, e-mail ou qualquer outra forma de comunicação que uma pessoa razoável consideraria apropriada nas circunstâncias.

A comunicação indireta será admitida quando: (i) a notificação direta provavelmente causar mais danos ao indivíduo afetado; (ii) a notificação direta provavelmente causar dificuldades indevidas para a organização; (iii) a organização não possui as informações de contato do indivíduo afetado. Essa comunicação deve ser dada por comunicação pública ou medida semelhante que poderia ser razoavelmente esperada para atingir os indivíduos afetados.

Conclusões e caminhos para a ANPD:

Tendo em vista a lógica da ANPD atuar como serviço e como plataforma, a existência de formulários claros e de uma plataforma de intermediação pode facilitar em diversos casos esses mecanismos de notificação. Podem inclusive estar automatizados no sistema.

No entanto, eles não abarcam todas as circunstâncias possíveis. Há situações em que pode ser difícil o contato com o titular. Nesse sentido, o objetivo da notificação é permitir que o titular tome decisões informadas sobre como tentar mitigar os riscos e danos que incidentes de segurança podem vir a ter. Para tal, **os meios a serem utilizados devem ser pensados no sentido de alcançar este objetivo, podendo ter múltiplos meios.**

Esse relatório contou com o generoso apoio financeiro do Reino Unido através de programa *Digital Access*

GREAT for PARTNERSHIP
BRITAIN & NORTHERN IRELAND

Acesse nossas redes

itsrio.org